14 *Sicherheit*

Ob Sie nun mit einem einzigen Computer oder in einem groûen Netzwerk arbeiten, Sie mössen den Faktor Sicherheit in Betracht ziehen. Unzureichende Sicherheitsvorkehrungen kðnnen zu Ausröstungs- oder Datenverlust föhren, vertrauliche Informationen kðnnten enthöllt oder wichtige Dateien modifiziert werden.

Man kðnnte sagen, daû der sicherste Computer in seiner Verpackung steckt. Dort ist er jedoch von wenig Nutzen. Denken Sie daran, daû die Benutzer durch verstÙrkte Sicherheitsmaûnahmen bei Aufgaben auf Sie angewiesen sind, die sie vorher selbst durchföhren konnten. Wenn sich herausstellt, daû der Unterstötzungsaufwand bei bestimmten Sicherheitsvorkehrungen öbermÙûig ist, sollten Sie die Sicherheit in Ihrem System etwas lockern, damit die Benutzer gewisse Aufgaben selbst erledigen kðnnen.

So integrieren Sie Sicherheitsvorkehrungen

Sicherheitsvorkehrungen treffen Sie beispielsweise, indem Sie Ihre Ausröstungselemente physisch sichern, den Zugriff auf bestimmte Verzeichnisse kontrollieren und die Benutzer daran hindern, bestimmte Aufgaben auszuföhren. Einige dieser Vorkehrungen betreffen sowohl Standalone-Computer als auch Computer in einem Netzwerk, wÙhrend andere nur Netzwerkverwalter interessieren werden.

Hinweis: Bei einigen Prozeduren in diesem Kapitel mössen Sie Befehle in ein Shell-Fenster eingeben,

wÙhrend Sie bei anderen die NetInfo-Datenbank modifizieren mössen. Mðchten Sie Shell-Befehle ausföhren, benðtigen Sie ª**root**º-Privilegien, wobei Sie manchmal den Befehl **su** verwenden kðnnen. HÙufig ist es jedoch notwendig, daû Sie sich als ª**root**º anmelden. Wenn Sie mit NetInfoManager eine NetInfo-Domain modifizieren, benðtigen Sie das ª**root**º-Paûwort för diese Domain.

Sicherheit bei Standalone-Computern

Die Sicherheitsvorkehrungen in diesem Abschnitt gelten sowohl för Standalone-Computer als auch för Computer in einem Netzwerk. Die Prozeduren in den Abschnitten ªPhysische Datensicherheitº und ªSchutz vor Virenº sollten von allen Systembenutzern beachtet werden Ð nicht nur vom Systemverwalter.

Physische Datensicherheit

Ein ausgewogenes Sicherheitssystem beginnt mit physischer Sicherheit. Computer sind am sichersten, wenn nur befugte Benutzer Zugang dazu haben. Ein physisch nicht sicherer Computer kann einfach fortgetragen werden. Somit haben Unbefugte Zugriff auf alle gespeicherten Daten.

Physische Sicherheit gilt auch för die Daten im Computer. Ihre Daten kðnnen Sie physisch am besten sichern, indem Sie sie aus dem Computer entfernen, wenn sie gerade nicht benðtigt werden. Speichern Sie Ihre Dokumente auf einer Wechselplatte, die Sie nach Gebrauch auswerfen. Vergessen Sie nicht, Ihre Platten an einem Ort aufzubewahren, der för Unbefugte unzugÙnglich ist.

Schutz vor Viren

Am hÙufigsten werden Computer öber Wechselplatten mit Viren oder anderen zerstðrenden Programmen infiziert. Eine andere Mðglichkeit ist Multimedia-E-Mail. Die meisten Viren schleichen sich mit Software ein, deren Herkunft zweifelhaft ist. Wenn Sie sich öber die Herkunft einer Anwendung nicht ganz sicher sind, sollten Sie sie deshalb nicht starten.

So schötzen Sie Verzeichnisse

Mehrere Verzeichnisse auf Ihrem NeXT-Computer werden in ganz besonderer Weise geschötzt Ð u. a. **/NextDeveloper/Demos**, **/usr/lib/NextStep/Displays** und ª/º (ªrootº). Alle Benutzer kðnnen dort Dateien oder Verzeichnisse ablegen, aber nur der Ersteller (oder ª**root**º) kann sie entfernen oder öberschreiben.

Obwohl dieses Schutzsystem för die Benutzer recht praktisch ist, ziehen Sie es eventuell vor, die Benutzer nicht in diese Verzeichnisse schreiben zu lassen. Wenn Sie den Schreibzugriff aufheben, mössen hier alle Dateien oder Verzeichnisse als ª**root**º erstellt werden. Bei **/usr/lib/NextStep/Displays** bedeutet dies, daû die Benutzer ohne Schreibzugriff selbst keine zusÙtzlichen Bildschirme an ihren Computer anschlieûen kðnnen.

So entziehen Sie die Schreibberechtigung

Folgendermaûen entziehen Sie die Schreibberechtigung för ein Verzeichnis:

1. Geben Sie den folgenden Befehl in ein Shell-Fenster ein. Ersetzen Sie dabei */verzeichnis* durch den Namen des Verzeichnisses, das Sie schötzen mðchten:

   chmod 755 */verzeichnis*

2. šberpröfen Sie die Wirksamkeit des Schutzes, indem Sie folgende Zeile eingeben:

   ls -ldg */verzeichnis*

   Daraufhin sollte etwa folgende Ausgabe erscheinen:

   ```
   drwxr-xr-x 16 root     wheel       1024 Oct  3 16:02 /verzeichnis
   ```

   Hinweis: Die erste Zeichenfolge dieser Ausgabe gibt die Berechtigungen för das Verzeichnis an und sollte Ihrer Ausgabe entsprechen. Die Angaben öber den Eigentömer und die Gruppe sollten auch identisch sein, der Rest kann jedoch unterschiedlich sein.

So stellen Sie die Schreibberechtigung wieder her

Mðchten Sie die Schreibberechtigung för ein bestimmtes Verzeichnis wiederherstellen, föhren Sie diese Schritte aus.

1. Geben Sie den folgenden Befehl in ein Shell-Fenster ein:

   chmod 1777 */verzeichnis*

2. šberpröfen Sie die neuen Berechtigungen, indem Sie folgende Zeile eingeben:

   ls -ldg */verzeichnis*

   Die Ausgabe sollte folgender Zeile Ùhneln:

   ```
   drwxrwxrwt 16 root     wheel       1024 Oct  3 16:02 /verzeichnis
   ```

So setzen Sie ein Hardware-Paûwort

Das Hardware-Paûwort ist eine einfache Methode, die Sicherheit Ihres Computers zu verbessern. Wurde ein Hardware-Paûwort gesetzt, benðtigen die Benutzer dieses Paûwort, um gewisse Funktionen auszuföhren. Das Paûwort ist z. B. erforderlich, um im Einzelbenutzer-Modus zu starten Ð wodurch der Benutzer ªrootº-Zugriff erhÙlt Ð oder um von einer anderen als der voreingestellten Platte aus zu starten Ð wodurch der Benutzer ebenfalls ªrootº-Zugriff erhalten kðnnte. Das Hardware-Paûwort sollten Sie, wie andere Paûwðrter auch, regelmÙûig wechseln. Weitere Einzelheiten zu diesem Thema finden Sie in Kapitel 9, ªHochfahren und Herunterfahren des Systemsº.

So entziehen Sie ºrootº-Privilegien för Preferences

Die Anwendung ªPreferencesº ermðglicht es Benutzern, zahlreiche Funktionen ihres Systems zu modifizieren. Einige dieser Modifikationen kðnnen nur mit ª**root**º-Privilegien erfolgreich ausgeföhrt werden. Mðchte ein Benutzer beispielsweise die Zeiteinstellung verÙndern, muû er den Wert Ùndern, der im Uhren-Schaltkreis gespeichert ist. Dazu benðtigt er ª**root**º-Zugriff. För alle Eingriffe, die ª**root**º-Zugriff erfordern, gibt es eine entsprechende Programmdatei in **/usr/lib/Preferences**. In diesem Verzeichnis finden Sie die Datei **boot_cmd**, mit der Sie das StartgerÙt Ùndern kðnnen, **check_ntpd**, mit der Sie die Zeit mit dem Netzwerk-Zeitdienst synchronisieren, und **clock_chip**, **date** sowie **set_time_zone**, mit der Sie Zeit, Datum und Zeitzone verÙndern

kðnnen.

Wenn Sie eine dieser Funktionen deaktivieren mðchten, kðnnen Sie die Berechtigungen für die entsprechende Datei in **/usr/lib/Preferences** Ùndern. Falls die Benutzer beispielsweise nicht berechtigt sein sollen, das StartgerÙt zu Ùndern, verÙndern Sie die Berechtigungen für **boot_cmd**.

Wenn Ihre Computer an ein Netzwerk angeschlossen sind, sollten Sie den Netzwerk-Zeitdienst immer aktivieren, damit die Zeit zentral eingestellt wird. Mit aktiviertem Netzwerk-Zeitdienst kðnnen die Benutzer das Datum und die Uhrzeit auf ihren lokalen Computern nicht selbst verÙndern Ð sie kðnnen sie lediglich mit der Netzwerk-Zeit synchronisieren. Das ist besonders wichtig, wenn Sie entfernte Dateien gemeinsam nutzen. Auûerdem werden auf diese Weise Probleme mit Programmen vermieden, bei denen Erstellungs- und …nderungszeitpunkt der Dateien eine Rolle spielen.

Wenn Sie keine Netzwerk-Zeit verwenden, kðnnen Sie die Berechtigungen für die Dateien **clock_chip**, **date** und **set_time_zone** Ùndern. Falls Sie hier die ª**root**º-Privilegien entziehen, kðnnen die Benutzer die Zeit nicht verÙndern.

So entziehen Sie ªrootº-Privilegien

Mit folgenden Schritten verhindern Sie, daû mit Preferences eine Funktion als ª**root**º ausgeföhrt wird.

1. Geben Sie die folgenden Befehle ein. Ersetzen Sie dabei *datei* durch den entsprechenden Dateinamen:

   ```
   cd /usr/lib/Preferences
   chmod 755 datei
   ```

2. šberpröfen Sie die Wirksamkeit des Schutzes, indem Sie folgenden Befehl eingeben. Ersetzen Sie *datei* wiederum durch den entsprechenden Dateinamen:

   ```
   ls -lg datei
   ```

   Daraufhin sollte eine Zeile Ùhnlich der folgenden angezeigt werden:

   ```
   -rwxr-xr-x  1 root   wheel   16384 Sep 19 21:08 datum*
   ```

So stellen Sie ªrootº-Privilegien wieder her

Mðchten Sie die ª**root**º-Privilegien för eine Funktion der Anwendung ªPreferencesº wiederherstellen, föhren Sie folgende Schritte aus.

1. Geben Sie die folgenden Befehle ein. Ersetzen Sie dabei *datei* durch den entsprechenden Dateinamen:

```
cd /usr/lib/Preferences
chmod 6755 datei
```

2. šberpröfen Sie die Wirksamkeit des Schutzes, indem Sie folgendes eingeben:

```
ls -lg datei
```

   Daraufhin sollte etwa folgende Zeile angezeigt werden:

```
-rwsr-sr-x  1 root   wheel   16384 Sep 19 21:08 datum*
```

So entziehen Sie ªrootº-Privilegien för PrintManager

In manchen FÙllen wird PrintManager ebenfalls mit ª**root**º-Privilegien ausgeföhrt. Auf diese Weise kðnnen alle Benutzer Drucker hinzufögen oder entfernen und Druckerwarteschlangen unterbrechen. Vielleicht mðchten Sie den Computer, der als gemeinsam genutzte Drucker-Ressource dient, nicht modifizieren lassen. In diesem Fall kðnnen Sie die Zugriffsberechtigungen för PrintManager Ùndern und die ª**root**º-Privilegien för die Anwendung deaktivieren.

So entziehen Sie ªrootº-Privilegien

Mit der folgenden Prozedur schrÙnken Sie die Funktionen von PrintManager ein.

1. Geben Sie folgende Befehle in ein Shell-Fenster ein:

```
cd /NextApps/PrintManager.app
chmod 755 PrintManager
```

2. šberpröfen Sie die Wirksamkeit des Schutzes, indem Sie folgenden Befehl eingeben:

```
ls -lg PrintManager
```

Daraufhin sollte eine Zeile Ùhnlich der folgenden erscheinen:

```
-rwxr-xr-x  1 root   wheel  163840 Sep 19 21:08 PrintManager
```

So stellen Sie ªrootº-Privilegien wieder her

Mit den folgenden Schritten stellen Sie die ª**root**º-Privilegien wieder her:

1. Geben Sie die folgenden Befehle ein:

```
cd /NextApps/PrintManager.app
chmod 6755 PrintManager
```

2. šberpröfen Sie die Wirksamkeit des Schutzes, indem Sie folgenden Befehl eingeben:

```
ls -lg PrintManager
```

Daraufhin sollte eine Zeile Ùhnlich der folgenden erscheinen:

```
-rwsr-sr-x  1 root   wheel  163840 Sep 19 21:08 PrintManager
```

So setzen Sie Sicherheitsoptionen in NetInfo

Es gibt vier verschiedene Optionen, mit denen Sie die Sicherheit Ihres Computers verbessern kðnnen. Sie aktivieren diese Optionen, indem Sie die NetInfo-Datenbank modifizieren. Hier werden die vier Optionen beschrieben:

- **login_accounting** Ð Wird diese Option gesetzt, generiert **syslog** för jeden miûlungenen Anmeldeversuch eine Meldung. Die Meldungen werden in **/usr/adm/messages** aufgezeichnet.
- **secure_passwords** Ð Mit dieser Option mössen Paûwðrter aus 8 Zeichen bestehen, und mindestens ein Zeichen darf kein Buchstabe sein.

- **lockout** Ð Diese Option fordert nach jedem miûlungenen Anmeldeversuch eine Wartezeit, bevor ein neuer Versuch gemacht werden kann. Die anfÙngliche Wartezeit ist 1 Sekunde. Jeder Fehlschlag verdoppelt die Wartezeit bis auf maximal 10 Minuten.
- **discourage_public_servers** Ð Falls Sie diese Option setzen, kðnnen die Benutzer weder den ðffentlichen Fenster-Server noch den ðffentlichen Sound-Server einstellen. Das Dialogfenster ªExpertenº der Anwendung ªPreferencesº enthÙlt för diese Optionen dann keine markierbaren KÙstchen.

Mðchten Sie eine Sicherheitsoption setzen, gehen Sie folgendermaûen vor:

1. Starten Sie NetInfoManager.
2. Doppelklicken Sie auf ª/º, um das Verzeichnisfenster zu ðffnen.
3. WÙhlen Sie im Menö ªVerzeichnisº den Befehl ªEigenschaft anfögenº, um eine neue Eigenschaft hinzuzufögen.
4. Geben Sie in das Textfeld **security_options** ein und dröcken Sie die Return-Taste.

F26.tiff ,

5. WÙhlen Sie im Menö ªVerzeichnisº den Befehl ªNeuer Wertº.
6. Geben Sie den Namen der gewönschten Sicherheitsoption ein (wie vorher beschrieben) und dröcken Sie die Return-Taste.

F27.tiff ,

7. Falls Sie weitere Optionen einstellen mðchten, wÙhlen Sie im Menö ªVerzeichnisº den Befehl ªWert anfögenº, geben den entsprechenden Namen ein und dröcken die Return-Taste.
8. WÙhlen Sie im Menö ªVerzeichnisº den Befehl ªSichernº.

Hinweis: Falls Sie mehrere Computer schötzen mðchten, kðnnen Sie diese Optionen in der Root-Domain oder in einer mittleren Domain setzen. Die dort gesetzten Sicherheitsoptionen sind dann för alle Computer göltig, die von dieser Domain bedient werden.

Sicherheit im lokalen Netzwerk

Falls Sie an ein lokales Netzwerk (LAN, Local Area Network) angeschlossen sind, kðnnten zusÙtzliche Sicherheitsmaûnahmen notwendig sein. Die nachfolgend aufgelisteten Vorkehrungen kðnnten selbst in einem kleinen, aus NeXT-Computern bestehenden Netzwerk nötzlich sein.

Die Sicherheit eines Netzwerkes kann mit der Festigkeit einer Kette verglichen werden: Die Kette ist so stark wie ihr schwÙchstes Glied. Um die Sicherheit eines Netzwerkes zu gewÙhrleisten, mössen *alle* angeschlossenen Computer gesichert sein. Werden die Sicherheitsvorkehrungen bei einem Computer vernachlÙssigt, entspricht dieser Computer dem rostigen Glied einer Kette Ð dort wird das Sicherheitssystem zusammenbrechen.

Wenn Sie die Sicherheit in Ihrem Netzwerk etwas lockerer handhaben wollen, sollten Sie vor allem bei externen Zugriffsrechten auf das Netzwerk vorsichtig sein. Sicherheitsprobleme entstehen meistens nicht innerhalb des Netzwerkes. Die Bedrohung kommt von auûen, öber Modems oder Verbindungen zu anderen Netzwerken. Sie vermeiden derartige Probleme, indem Sie die Modems und Netzwerkverbindungen sicherer gestalten.

Allgemeine Vorsichtsmaûnahmen

Im Netzwerkbetrieb sollten Sie besonders för die Sicherheit der gemeinsam benutzten Dateisysteme sorgen. šberlegen Sie sich sehr sorgfÙltig, welche Computer ª**root**º-Zugriff auf ein gemeinsam benutztes Verzeichnis haben sollen. ErwÙgen Sie auch genau, wie unbekannte Benutzer behandelt werden sollen. Weitere Einzelheiten zu diesem Thema finden Sie in Kapitel 4, ªSo richten Sie NFS (Network File System) einº.

Eine andere grundlegende Sicherheitsvorkehrung betrifft die Optionen ª–ffentlicher Fenster-Serverº und ª–ffentlicher Sound-Serverº im Bereich ªExperten-PrÙferenzenº der Anwendung ªPreferencesº. In der Voreinstellung sind beide Optionen aus Sicherheitsgrönden deaktiviert. Werden sie aktiviert, kðnnen entfernte

Benutzer Tonaufzeichnungen auf Ihrem Computer abspielen, öber Ihr Mikrofon mithðren, auf Ihrem Bildschirm zeichnen, Ihre Bildschirmanzeige lesen oder Ihren Digital-Signal-Prozessor (DSP) verwenden.

Der letzte Aspekt allgemeiner Sicherheitsvorkehrungen in einem Netzwerk betrifft grundlegende UNIX-Sicherheitsmaûnahmen. In der Voreinstellung trauen die Shells des Betriebssystems auf NeXT-Computern (etwa **/bin/csh**) keiner Information, die von anderen Computern im Netzwerk kommt. Vielleicht sind Sie der Meinung, Computer sollten einander vertrauen, damit alle Benutzer sich frei im Netzwerk bewegen kðnnen. Bevor Sie diese Mðglichkeiten verwenden, lesen Sie im UNIX-Handbuch die Abschnitte öber **.rhosts** und **hosts.equiv** sorgfÙltig durch. Wenn Sie einem anderen Computer vertrauen wollen, mössen Sie för diesen Computer die gleichen Sicherheitsmaûnahmen wie för Ihren eigenen Computer einstellen. Falls dies nicht beachtet wird, steht die Hintertör weit offen.

So sichern Sie das Hinzufögen von Druckern und FaxgerÙten

Sie kðnnen normale Benutzer daran hindern, Drucker oder Faxmodems hinzuzufögen oder sie zu entfernen. Zu diesem Zweck deaktivieren Sie die Mðglichkeit, die NetInfo-Verzeichnisse **printers** und **fax_modems** zu modifizieren. Der Nachteil solch strenger Sicherheitsmaûnahmen ist, daû die Benutzer ihre Drucker nicht ohne Ihre Hilfe mit den öbrigen Netzwerkbenutzern gemeinsam nutzen kðnnen.

Die folgenden Prozeduren mössen för alle Domains durchgeföhrt werden, die Sie schötzen mðchten.

So deaktivieren Sie die Modifikationsberechtigung

Mit den folgenden Prozeduren hindern Sie Benutzer daran, dem Netzwerk Drucker oder Faxmodems hinzuzufögen oder sie zu entfernen.

1. Starten Sie NetInfoManager und ðffnen Sie die Domain, die Sie schötzen mðchten.
2. Klicken Sie im Domainfenster auf **/printers**.

F0.tiff ,

3. Doppelklicken Sie auf **printers**, um ein Verzeichnisfenster zu öffnen. Klicken Sie danach auf _**writers**.

F1.tiff ,

Mit den Werten der Eigenschaft _**writers** werden die Namen der Benutzer aufgelistet, die den Inhalt dieses NetInfo-Verzeichnisses modifizieren dörfen Ð d. h. Eigenschaften hinzufögen, lðschen oder modifizieren und Unterverzeichnisse hinzufögen oder lðschen. In diesem Fall besagt ª*****º, daû jeder Benutzer Modifikationen vornehmen darf.

4. Entfernen Sie diese Eigenschaft, indem Sie im Menö ªBearbeitenº den Befehl ªLðschenº wÙhlen.
5. WÙhlen Sie im Menö ªVerzeichnisº den Befehl ªSichernº, um Ihre …nderungen zu sichern. Wenn ein BestÙtigungsfenster erscheint, klicken Sie auf ªVerÙndernº.

F28.tiff ,

6. Geben Sie das ª**root**º-Paûwort för diese Domain ein, falls Sie dazu aufgefordert werden.

Jetzt kann nur noch ª**root**º dieses Verzeichnis erstellen, lðschen oder modifizieren. Wiederholen Sie diese Prozedur auf Wunsch för das Verzeichnis **/fax_modems**.

So aktivieren Sie die Modifikationsberechtigung

Mðchten Sie die urspränglichen Berechtigungen wiederherstellen, mössen Sie die Eigenschaft _**writers** neu erstellen.

1. Starten Sie NetInfoManager.
2. Doppelklicken Sie auf **/printers**, um das Verzeichnisfenster zu öffnen.

F2.tiff ,

3. WÙhlen Sie im Menö ªVerzeichnisº den Befehl ªEigenschaft anfögenº.

F3.tiff ,

4. …ndern Sie im Textfeld **new_property** auf _**writers** ab und dröcken Sie anschlieûend die Return-Taste, um die …nderung zu registrieren.

F4.tiff ,

5. WÙhlen Sie im Menö ªVerzeichnisº den Befehl ªNeuer Wertº.

F5.tiff ,

6. Geben Sie in das Textfeld ª*º ein und dröcken Sie die Return-Taste.

F6.tiff ,

7. Sichern Sie das Verzeichnis, indem Sie im Menö ªVerzeichnisº den Befehl ªSichernº wÙhlen. Falls ein BestÙtigungsfenster erscheint, klicken Sie auf ªVerÙndernº.
8. Geben Sie das ª**root**º-Paûwort för die Domain ein, falls Sie dazu aufgefordert werden.

Jetzt kðnnen alle Benutzer wieder Modifikationen an diesem Verzeichnis vornehmen. Die gleiche Prozedur gilt auch för das Verzeichnis /**fax_modems**.

So sichern Sie DruckauftrÙge

Sie kðnnen DruckauftrÙge vom nicht-privilegierten Benutzer **nobody** ausföhren lassen (dem Account, mit dem unbekannte Benutzer auf ein NFS-Verzeichnis zugreifen). Dazu mössen Sie dem NetInfo-Eintrag för den Drucker die Eigenschaft **RemoteAsNobody** hinzufögen. Diese Eigenschaft benðtigt keinen Wert, sie muû nur vorhanden sein.

So werden DruckauftrÙge als ªnobodyº ausgeföhrt

Mðchten Sie DruckauftrÙge als **nobody** ausföhren, gehen Sie folgendermaûen vor:

1. Starten Sie NetInfoManager und ðffnen Sie die Domain, die Sie schötzen mðchten.
2. Klicken Sie erst auf **/printers** und danach auf den Namen eines bestimmten Druckers. Doppelklicken Sie anschlieûend auf den Namen, um das Verzeichnisfenster zu ðffnen.
3. Klicken Sie auf **name** und wÙhlen Sie anschlieûend im Menö ªVerzeichnisº den Befehl ªEigenschaft anfögenº. Daraufhin erscheint eine neue Eigenschaft mit dem Namen **new_property**.

F7.tiff ,

4. Geben Sie in das Textfeld **RemoteAsNobody** ein und dröcken Sie die Return-Taste.

F8.tiff ,

5. WÙhlen Sie im Menö ªVerzeichnisº den Befehl ªSichernº, um Ihre …nderungen zu sichern. Falls daraufhin ein BestÙtigungsfenster erscheint, klicken Sie auf ªVerÙndernº.
6. Geben Sie das ª**root**º-Paûwort för die Domain ein, falls Sie dazu aufgefordert werden.

Hinweis: Mðchten Sie verhindern, daû jemand die Eigenschaft **RemoteAsNobody** entfernt, mössen Sie die Eigenschaft _**writers** lðschen.

So werden DruckauftrÙge vom Benutzer ausgeföhrt

Mðchten Sie diese Prozedur röckgÙngig machen, lðschen Sie einfach die Eigenschaft **RemoteAsNobody**. Eventuell mðchten Sie gleichzeitig die Eigenschaft _**writers** wieder hinzufögen. Folgen Sie dazu den Anweisungen im vorherigen Abschnitt, ªSo sichern Sie das Hinzufögen von Druckern und FaxgerÙtenº.

1. Starten Sie NetInfoManager und ðffnen Sie die entsprechende Domain.
2. Klicken Sie erst auf **/printers** und danach auf den Namen eines Druckers. Doppelklicken Sie anschlieûend auf den Namen, um das Verzeichnisfenster zu ðffnen.
3. Klicken Sie auf **RemoteAsNobody**.

F9.tiff ,

4. WÙhlen Sie im Menö ªBearbeitenº den Befehl ªLðschenº.

F10.tiff ,

5. WÙhlen Sie im Menö ªVerzeichnisº den Befehl ªSichernº. Falls ein BestÙtigungsfenster erscheint, klicken Sie auf ªVerÙndernº. Geben Sie das ª**root**º-Paûwort ein, falls Sie dazu aufgefordert werden.

So öberpröfen Sie Paûwðrter

Am einfachsten öberpröfen Sie die Paûwðrter auf einem Computer mit NetInfoManager.

1. Melden Sie sich bei dem Computer an, auf dem die Accounts gespeichert sind, die Sie öberpröfen mðchten.
2. Starten Sie NetInfoManager und ðffnen Sie die Domain, die Sie öberpröfen wollen.
3. Klicken Sie erst auf **/users** und anschlieûend auf eines der Unterverzeichnisse.

F11.tiff ,

4. WÙhlen Sie im Menö ªDomainº den Befehl ªšbersichtº und anschlieûend ªVerzeichnisse einsehen nach ...º. Klicken Sie im daraufhin angezeigten Dialogfenster auf **passwd**.

F12.tiff ,

5. Klicken Sie auf ªšbersicht einstellenº.

   Die Verzeichnisse werden jetzt im Domainfenster nach dem Wert ihrer Eigenschaft **passwd** aufgelistet und nicht mehr nach dem Wert ihrer Eigenschaft **name**.

6. Suchen Sie nach Accounts, die kein Paûwort haben. Diese Accounts haben entweder keinen Wert oder sind durch **dir:**# gekennzeichnet, wobei # durch eine Zahl ersetzt wird.

F13.tiff ,

7. Klicken Sie auf ein Unterverzeichnis, das kein Paûwort hat. Doppelklicken Sie anschlieûend darauf, um das Verzeichnisfenster zu ðffnen.

F14.tiff ,

8. WÙhlen Sie die Eigenschaft **name**. Der Name des Benutzers erscheint in der zweiten Spalte.
9. Bitten Sie den Benutzer, mit Preferences ein Paûwort hinzuzufögen, oder fögen Sie selbst eines mit UserManager hinzu. SpÙter sollte es der Benutzer Ùndern.

Wiederholen Sie diese Schritte för jede Domain.

So finden Sie die Programme ªsetuidº und ªsetgidº

Alle Programme, einschlieûlich der Shell-Skripte, kðnnen so konfiguriert werden, daû sie als Eigentömer der Programmdatei anstelle des tatsÙchlichen Benutzers ausgeföhrt werden. Derartige Programmdateien werden *setuid-Dateien* genannt, weil sie das Benutzer-ID (UID) setzen. Programme kðnnen auch so konfiguriert werden, daû sie mit den Privilegien der Gruppe ausgeföhrt werden, die dieser Datei zugeordnet ist Ð und nicht mit den Privilegien der voreingestellten Gruppe des Benutzers. Dabei handelt es sich um die sogenannten *setgid-Dateien*.

Zahlreiche Programme kðnnen so als **ªrootº** oder als **wheel** ausgeföhrt werden. Die meisten dieser Programme wurden sorgfÙltig getestet und sind sicher. Installieren Sie jedoch ein Programm oder eine Anwendung mit dieser Funktion, sollten Sie vorsichtig sein. Shell-Skripte, die so konfiguriert wurden, daû sie als **ªrootº** ausgeföhrt werden, kðnnten z. B. verwendet werden, um das Sicherheitssystem Ihres Computers zu umgehen.

Um alle setuid-Dateien zu finden, geben Sie folgenden Befehl in ein Shell-Fenster ein:

```
find / -perm -4000 -print
```

Wenn Sie die Ausgabe auf Dateien beschrÙnken mðchten, die das Benutzer-ID auf **ªrootº** setzen, verwenden Sie den folgenden Befehl:

```
find / -perm -4000 -user root -print
```

Mit Ùhnlichen Befehlen kðnnen Sie alle setgid-Dateien oder die Dateien finden, die das Gruppen-ID auf eine bestimmte Gruppe setzen. Einzelheiten finden Sie im UNIX-Handbuch unter **find**.

Wenn Sie derartige Dateien finden, kðnnen Sie sie entweder lðschen oder die setuid- bzw. die setgid-Bits mit dem Befehl **chmod** aus der Datei entfernen. Ein Beispiel hierför ist der Befehl, der weiter vorne in diesem Kapitel verwendet wurde, um die Berechtigungen zu sichern. Weitere Informationen finden Sie im UNIX-Handbuch unter **chmod**.

Eine weitere Sicherheitsvorkehrung in diesem Zusammenhang besteht darin, das setuid-Bit zu ignorieren, wenn Sie den ªmountº för entfernte Verzeichnisse durchföhren (d. h. die Verzeichnisse importieren). Einzelheiten hierzu finden Sie im Kapitel 4, ªSo richten Sie NFS (Network File System) einº.

Sicherheit und entfernter Zugriff

šberwachen Sie insbesondere die Computer, die externen Zugriff gewÙhren. Externer Zugriff kann technisch Ùuûerst raffiniert sein, wie etwa Hochgeschwindigkeitsöbertragungen von Daten öber ein TCP/IP-Weitbereichsnetz, Internet genannt. Er kann aber auch ganz einfach öber ein Modem geschehen, mit dem Sie Ihren Computer entfernt verwenden kðnnen. Die Sicherung komplexer Netzwerkanlagen kann eine sehr verwickelte Sache sein. Hier werden ein paar grundlegende Schritte erlÙutert, die Sie beachten sollten, wenn Sie entfernten Zugriff auf Ihr lokales Netzwerk gewÙhren:

- Die Benutzer des Computers, der an das Modem oder das externe Netzwerk angeschlossen ist, mössen regelmÙûig ihr Paûwort Ùndern. Dies gilt auch för die Benutzer, die Computer im ganzen Netzwerk verwenden. Alle Accounts mössen öber Paûwðrter verfögen.
- šberwachen Sie den Computer besonders sorgfÙltig, der an das Modem oder das externe Netzwerk angeschlossen ist, damit Sie Eindringlinge schnell erkennen kðnnen.
- Konfigurieren Sie die Dateien **.rhosts** und **hosts.equiv** so, daû die anderen Computer im Netzwerk dem Computer nicht vertrauen, der an ein externes Netzwerk oder ein Modem angeschlossen ist. Im UNIX-Handbuch finden Sie weitere Informationen hierzu.
- Entscheiden Sie, welche Dienste einem externen Netzwerk zur Verfögung gestellt werden sollen Ð wie etwa Mail, Zugriff auf entfernte Dateien oder entfernte Anmeldungen. Alle anderen Dienste sollten deaktiviert werden, damit Sie sich um deren Sicherheit nicht sorgen mössen.
- Sollten Sie UUCP-Verbindungen einrichten, finden Sie Einzelheiten öber Sicherheitsvorkehrungen in Kapitel 12, ªSo verwenden Sie UUCPº.
- BeschrÙnken Sie den Zugriff auf NetInfo-Domains. Föhren Sie dazu die Prozeduren im folgenden Abschnitt aus.

So richten Sie Zugriffskontrollen för eine NetInfo-Domain ein

Wenn Ihr NeXT-Computer (oder Ihr Netzwerk) externen Zugriff von einem anderen TCP/IP-Netzwerk aus

gewÙhrt, sollten Sie den Zugriff auf die Verwaltungsdaten in NetInfo einschrÙnken. Diese Daten öber Hosts und Benutzer in NetInfo kðnnten verwendet werden, um die Sicherheit Ihres Netzwerkes zu beeintrÙchtigen. Paûwðrter sind beispielsweise durch Programme gefÙhrdet, die darauf abzielen, ein Paûwort zu ermitteln. Alle Domains, in denen Benutzer-Paûwðrter gespeichert sind, sollten gegen externen Zugriff geschötzt werden. Zu diesem Zweck kann eine Eigenschaft erstellt werden, in der die Internet-Adressen der Netzwerke aufgelistet werden, denen der Zugriff auf die NetInfo-Domain gewÙhrt wird.

SimpleNetworkStarter erstellt diese Eigenschaft in der Root-Domain, wenn Sie Ihr Netzwerk einrichten. Dazu muû aber das KÙstchen ªZugriff auf Netzwerk-Verwaltungsdaten auf das lokale Netzwerk beschrÙnkenº markiert sein. Sie kðnnen mit SimpleNetworkStarter auch eine lokale Domain schötzen, indem Sie auf den Schalter ªDiesen Host konfigurierenº klicken. In der Voreinstellung sichert SimpleNetworkStarter diese Domain. Wenn Sie Ihr Netzwerk nicht mit SimpleNetworkStarter konfiguriert haben oder wenn Sie die Liste der Netzwerke Ùndern mðchten, denen vertraut wird, folgen Sie den Prozeduren im nÙchsten Abschnitt.

So schötzen Sie eine Domain

Mðchten Sie den Zugriff auf eine Domain einschrÙnken, gehen Sie folgendermaûen vor:

1. Starten Sie NetInfoManager und ðffnen Sie die Domain, die Sie schötzen mðchten.
2. Klicken Sie auf ª/º.

F15.tiff ,

3. Doppelklicken Sie auf ª/º, um ein Verzeichnisfenster zu ðffnen.

F16.tiff ,

4. Klicken Sie in der Spalte ªEigenschaftenº auf **master** und wÙhlen Sie anschlieûend im Menö ªVerzeichnisº den Befehl ªEigenschaft anfögenº.

F17.tiff ,

5. Geben Sie in das Textfeld **trusted_networks** ein und dröcken Sie die Return-Taste, um die …nderung zu registrieren.

F18.tiff ,

6. WÙhlen Sie im Menö ªVerzeichnisº den Befehl ªNeuer Wertº.

F19.tiff ,

7. Klicken Sie in der Spalte ªWerteº auf **new_value**. Geben Sie Ihre Netzwerkadresse in das Textfeld ein. Die Netzwerkadresse ist der Teil der Internet-Adresse, mit der Ihr Netzwerk identifiziert wird. Einzelheiten hierzu finden Sie im Anhang C, ªInternet-Adressierungº.

Warnung: Geben Sie die Nummer sehr sorgfÙltig ein. Ein Fehler kann Ihr Netzwerk deaktivieren. Der Netzwerknummer darf kein Punkt folgen (z. B.: **192.42.172** und nicht **192.42.172.**).

8. Dröcken Sie die Return-Taste, um die …nderung zu registrieren.

F20.tiff ,

9. Sichern Sie das Verzeichnis, indem Sie im Menö ªVerzeichnisº den Befehl ªSichernº wÙhlen. Falls ein BestÙtigungsfenster erscheint, klicken Sie auf ªVerÙndernº. Geben Sie das ª**root**º-Paûwort ein, falls Sie dazu aufgefordert werden.

Jetzt kðnnen nur noch die Computer des angegebenen Netzwerkes auf diese Domain zugreifen.

So entfernen Sie die ZugriffsbeschrÙnkungen för eine Domain

Falls Sie noch anderen Netzwerken Zugriff gewÙhren mössen, fögen Sie deren Netzwerkadressen einfach der Eigenschaft **trusted_networks** hinzu. Wenn Sie auf die Domain unbeschrÙnkten Zugriff gewÙhren wollen, gehen Sie folgendermaûen vor:

1. Starten Sie NetInfoManager und öffnen Sie die entsprechende Domain.
2. Klicken Sie auf ª/º.

F21.tiff ,

3. Doppelklicken Sie auf ª/º, um das Verzeichnisfenster zu öffnen. Klicken Sie danach in der Spalte ªEigenschaftenº auf **trusted_networks**.

F23.tiff ,

4. WÙhlen Sie im Menö ªBearbeitenº den Befehl ªLöschenº.

F24.tiff ,

Warnung: Falls Sie versehentlich die Eigenschaft **master** löschen, schlieûen Sie das Verzeichnisfenster, ohne die … nderungen zu sichern. Ohne eine Eigenschaft **master** funktioniert die Domain nicht.

5. Sichern Sie die …nderungen, indem Sie im Menö ªVerzeichnisº den Befehl ªSichernº wÙhlen. Falls ein BestÙtigungsfenster erscheint, klicken Sie auf ªVerÙndernº. Geben Sie das **ªrootº**-Paûwort ein, falls Sie dazu aufgefordert werden.

So öberwachen Sie die BenutzeraktivitÙten

Mðchten Sie wissen, welche Benutzer sich wie lange bei Ihrem Computer angemeldet haben, verwenden Sie am einfachsten den Befehl **ac**. Mit folgendem Befehl erhalten Sie eine Liste der Benutzer mit Angabe der Benutzungsdauer des Systems:

```
/usr/etc/ac -p
```

In der Ausgabe werden alle Benutzer in ungeordneter Reihenfolge und unter Angabe der Benutzungsdauer aufgelistet, die sich seit der letzten Röckstellung der Abrechnung angemeldet haben. Um die Abrechnung zuröckzustellen, geben Sie folgenden Befehl ein:

```
cat /dev/null > /private/adm/wmtp
```

Damit werden alle Abrechnungsdaten gelðscht, und der ZÙhler wird zuröckgestellt.

Bei der šberwachung der BenutzeraktivitÙten sollten Sie auf zwei Dinge achten:

- Nicht erkannte Accounts
- Ungewðhnlich starke AktivitÙt eines bestimmten Accounts

Mit dem folgenden Befehl kðnnen Sie ungefÙhr die letzten 20 Anmeldungen öberpröfen:

```
last | head -20
```

Unter anderem enthÙlt die Ausgabe den Namen des Benutzers, den Anmeldezeitpunkt sowie die Benutzungsdauer. Suchen Sie vor allem nach Personen, die sich zu ungewðhnlichen Zeitpunkten oder von einem ungewðhnlichen Ort aus angemeldet haben. Mðchten Sie alle Anmeldungen seit der letzten Röckstellung des Systems auflisten, geben Sie den folgenden Befehl ein:

```
last
```

Diesen Befehl kðnnen Sie auch verwenden, um die verschiedenen Zeitpunkte zu öberpröfen, zu denen ein bestimmter Benutzer sich angemeldet hat.

Einzelheiten zu diesem Thema finden Sie im UNIX-Handbuch unter **ac** und **last**.

So garantieren Sie dauerhafte Sicherheit

Jedes Computer-Betriebssystem hat konzeptuelle MÙngel, die ausgenutzt werden kðnnen, um Sicherheitsvorkehrungen zu umgehen. Sie kðnnen die Sicherheit Ihres Computers und Ihres Netzwerkes wahren, indem Sie neu aufgetretene Probleme verfolgen und versuchen, sie in Zukunft zu vermeiden.

Verschiedene Organisationen informieren Computer-Besitzer öber mðgliche Sicherheitsprobleme. Sie kðnnen sich beispielsweise einer NeXT-Benutzergruppe anschlieûen und sind auf diese Weise in Sachen Sicherheit immer auf dem neusten Stand. Auûerdem haben Sie so eine ausgezeichnete Mðglichkeit, stets öber neue Entwicklungen informiert zu werden. Wenn Sie eine Liste der NeXT-Benutzergruppen erhalten mðchten, rufen Sie folgende Nummer an: 1-800-848-NeXT.