Prüfung von Linux unter datenschutzrechtlichen Gesichtspunkten

Während viele DSB mit Windows-Systemen gut zurechtkommen, gibt es Vorbehalte gegenüber Linux. Am Beispiel eines Debian-Linux-Systems schauen wir uns an, was Sie einfach herausfinden können, z.B. wo können Daten durch Sicherheitslücken nach außen gelangen, wo wird was protokolliert, wie verhält es sich mit Zugriffsrechten.

Bei der Beschäftigung mit einem Linux-System gilt es einige Grundfragen zu beantworten: Wie präsentiert sich z.B. das System im Netz, d.h. welche Dienste (Ports) sind von außen sichtbar? Welche Programme (Prozesse) laufen auf dem System? Wie sind Voreinstellungen konfiguriert, etwa für Dateizugriffsrechte? Was wird wo protokolliert?

Die erste Möglichkeit, sich einem System zu nähern, ist ein Portscan. Dabei wird mit einem Programm, z.B. nmap oder GFI Languard, versucht, festzustellen, welche Dienste auf einem Rechner im Netz angeboten werden. Abbildung 1 zeigt das typische Ergebnis eines Portscans mit nmap: Es finden sich Dienste, die nicht benötigt werden. Hier müssen Sie der Frage nachgehen, warum dieser oder jener Dienst überhaupt läuft.

Läuft der Server im internen Netz oder in der DMZ (Demilitarisierte Zone), also hinter einer Firewall, ist es sinnvoll, den Portscan von außen, d.h. vor der Firewall, zu wiederholen. Damit erkennt man, wie der Server von Unternehmensfremden gesehen wird.

Was wird gestartet?

Linux hat einen relativ einfachen Startmechanismus. Zuerst wird `/etc/init` bzw. `/sbin/init` gestartet und abgearbeitet. Dieser Prozess erhält die ID (PID) 1 und arbeitet `/etc/inittab` ab sowie die Skripte in `/etc/init.d`. Letztere werden aber nicht alle abgearbeitet: Im Verzeichnis `/etc/rcX.d` liegen Verknüpfungen, die angeben, welche Dateien für den Start in einem bestimmten Runlevel (Betriebsmodus) benötigt werden. Der aktuelle Runlevel (Wert zwischen 1 und 6, muss für das X im Verzeichnisnamen eingesetzt werden) kann durch das Kommando Runlevel angezeigt werden. Details zu den Startmechanismen findet man z.B. in der c't (Erik Heim, A long way $HOME: Wie Init-Skripte das System konfigurieren, c't 12/1999, Seite 174).

Eine Besonderheit bietet der Internet-Daemon inetd. Dieser Dienst „lauscht" am Netz und startet bei Bedarf die benötigten Programme. Er wird über die Dateien `/etc/services` und `/etc/inetd.conf` konfiguriert. Über die Datei `/etc/services` wird den TCP- und UDP-Ports eine Dienstbezeichnung zugeordnet und dann über diese Dienstbezeichnung in der `/etc/inetd.conf` das zu startende Programm festgelegt. So können Sie nachvollziehen, welche Programme beim Systemstart anlaufen.

```
Output
Interesting ports on  (192.168.1.2):
(The 1591 ports scanned but not shown below are in state: closed)
Port        State       Service
9/tcp       open        discard
13/tcp      open        daytime
22/tcp      open        ssh
25/tcp      open        smtp
37/tcp      open        time
110/tcp     open        pop-3
111/tcp     open        sunrpc
113/tcp     open        auth
515/tcp     open        printer
1024/tcp    open        kdm
Remote operating system guess: Linux 2.1.19 - 2.2.20
Uptime 0.003 days (since Sat Apr 10 12:15:17 2004)
```

Abbildung 1: Ob alle diese Dienste (discard, daytime, time, printer, kdm, sunrpc) auf einem POP3/SMTP-Mailserver benötigt werden, darf in Frage gestellt werden. Dargestellt ist das Ausgabefenster von nmap.

Was läuft?

Auf einem Linux-System laufen im Hintergrund viele Prozesse. Mithilfe des Kommandos `ps -ax` können Sie sich eine Liste anzeigen lassen. Ist unklar, wozu die einzelnen Programme erforderlich sind bzw. was ihre Funktion ist, sollte der DSB zuerst mit dem Administrator reden. Empfehlenswert ist darüber hinaus eine Recherche im Internet.

Wo wird protokolliert?

Die Protokolldateien befinden sich im Verzeichnis `/var/log`, entweder direkt in der Hauptprotokolldatei `/var/log/messages` oder in programmspezifischen Dateien. Es handelt sich um Textdateien, die mit jedem Editor gelesen werden können. Die Logdateien sind defaultmäßig für jedermann lesbar, d.h. die Unix-Dateiattribute sind rw-r--r--. Diese sind auf rw------- zu ändern, damit nur der Systemverwalter die Logdateien lesen kann. Der Besitzer und die Gruppe sind normalerweise root.

Außerdem sind durch entsprechende Einstellungen die Logeinträge möglichst zeitnah zu löschen. Eine Aufbewahrung von maximal sieben Tagen sollte für Fehlersuche und -behebung ausreichen. Für alle anderen Zwecke sind diese Dateien definitiv tabu.

In der Log-Datei `/var/log/messages` protokolliert ein Linux-System viele Systemereignisse genau mit (siehe Abbildung 3). Im abgebildeten Ausschnitt z.B. ändert der Administrator (root) um 20:14 am 24.03. sein Passwort. Danach wechselt der Benutzer user1 mit dem Befehl su in den Administrator-Account. Um 12.31 am 27.03. meldet sich der Benutzer user1

```
Mar 4 15:06:13 server.testnet.de sendmail[237]: PAA00237:
from=user1@testnet.de, size=1031, class=0, pri=31031, nrcpts=1,
msgid=<200403041400.PAA00237@server.testnet.de>,
relay=root@localhost
Mar 4 15:06:13 server.testnet.de sendmail[237]: PAA00237:
to=user2@testnet.de, ctladdr=root (0/0), delay=00:06:11,
xdelay=00:00:00, mailer=local, stat=Sent
```

Abbildung 2: Das Versenden einer E-Mail erzeugt auf dem Mailserver zwei Einträge in die entsprechende Protokolldatei. Hier ist ersichtlich, wer (user1@testnet.de) wem (user2@testnet.de) wann (4. März 2004 15:06) eine wie große (1031 Bytes) E-Mail geschickt hat.

vom Rechner 192.168.0.2 mittels telnet an. Um 21:10 erfolgt wieder eine Anmeldung des Benutzers user1 vom Rechner 192.168.0.2, diesmal aber per Secure Shell (SSH). Dabei erfolgt die Authentifizierung des Benutzers

```
Mar 24 20:14:08 server passwd[2479]: password for `root' changed by `root'
Mar 24 22:27:34 server su: (to root) user1 on /dev/tty2
Mar 27 12:31:33 server in.telnetd[169]: connect from user1@192.168.0.2
Mar 27 21:10:04 server opensshd[421]: Accepted rsa for user1 from 192.168.0.2 port 114
Mar 27 22:07:20 server popper[822]: connect from 192.168.0.2
Mar 27 22:07:20 server popper[822]: Stats: user1 1 725 0 0 client1 192.168.0.2
```

Abbildung 3: Einige beispielhafte Zeilen aus der Logdatei

über einen gültigen RSA-Schlüssel (private Key), nicht über ein Passwort. In den beiden letzten Zeilen holt der user1 per POP3-Protokoll seine E-Mail (1 Mail mit 725 Bytes) ab.

Es zeigt sich, dass mit geeigneten Auswertungswerkzeugen oft auch per Hand Etliches an sensibler Information aus dieser Logdatei gezogen werden kann.

Erwähnenswert ist auch die binäre Datei `/var/log/wtmp`. Sie kann mit dem Befehl `who/var/log/wtmp` angezeigt werden. Hier lässt sich genau nachvollziehen, wer sich wann von wo aus am System angemeldet hat.

Zugriffsrechte auf Benutzerdateien und Logdateien

Die Auswertung der Logdateien sagt viel über die Systemnutzung. Teilweise unterliegt die Information in den Logdateien dem Fernmeldegeheimnis. Deshalb ist der richtige Zugriffschutz auf diese Dateien wichtig. Während der Benutzer root uneingeschränkt alle Rechte hat, können Benutzern unter Linux Rechte entzogen werden. Jede Datei ist einem Benutzer und einer Gruppe zugeordnet. Für den Benutzer, für die Gruppe und für alle anderen können die Rechte ausführen (x), schreiben (w) und lesen (r) eingestellt werden. Die Dateirechte werden in drei Gruppen zu drei Zeichen angeben. Von links nach rechts: die drei Attribute für den Benutzer, dann die für die Gruppe und dann für den Rest. Ist das Recht gesetzt, wird der Buchstabe angegeben (maximal rwx), sonst ein Strich (keine Rechte, also ---).

Eine häufige, aber nicht datenschutzgerechte Voreinstellung für Rechte einer vom Benutzer angelegten Datei ist rw-r--r--. Damit können alle Benutzer des Systems die Datei lesen. Eine datenschutzgerechte Voreinstellung ist rw-------, da dann der Benutzer aktiv werden muss, um anderen Lese- oder Schreibrechte zu geben.

Auch im Verzeichnis `/etc` haben viele Konfigurationsdateien zu „offene“ Rechte. Es gibt allerdings nur wenig Software, die sich weigert, eine Konfigurationsdatei zu verwenden, wenn die Rechte zu großzügig gesetzt sind.

Fazit

Der Datenschutzbeauftragte hält fest, welche Programme auf einem Linux-System laufen, welche Benutzer und Gruppen es gibt und wie die wichtigsten Voreinstellungen lauten. Auf Basis dieser Informationen diskutiert er mit dem Administrator, ob bzw. wozu die Programme, Benutzer und Gruppen notwendig sind. Erfahrungsgemäß laufen z.B. auf vielen Rechnern Programme, die nicht benötigt werden, und es gibt noch Benutzerkonten von Benutzern, die das Unternehmen längst verlassen haben.

Möchten Sie sich noch intensiver mit der Prüfung von Linux oder anderen Betriebssystemen auseinandersetzen, empfehlen wir Ihnen das Praxishandbuch „IT-Know-how für den Datenschutzbeauftragten“ (www.interest.de/produkte/7530.html). Ausführliche Informationen zum Thema Verschlüsselung finden Sie z.B. bei R. W. Gerling, Verschlüsselung im betrieblichen Einsatz, Frechen 2000.

Autor: Rainer W. Gerling

Zum Autor: Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der FH München.

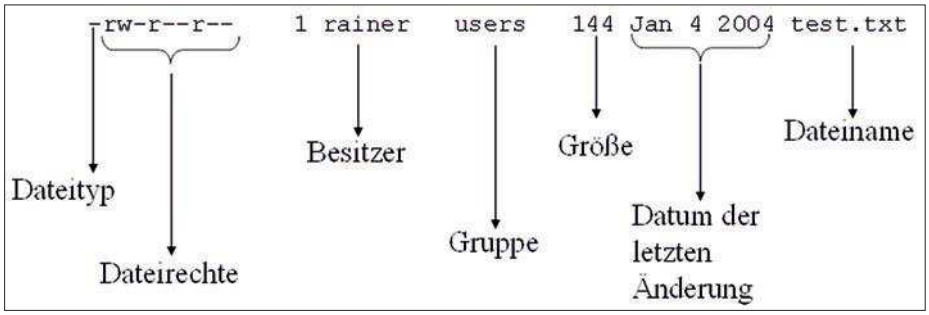

Abbildung 4: Die Bedeutung der Anzeige des Kommandos ls -ali. Für Dateityp wird angeben: „-“ normale Datei, „d“ Verzeichnis, „l“ symbolischer Link, „b“ blockorientierte Datei, „c“ zeichenorientierte Datei.