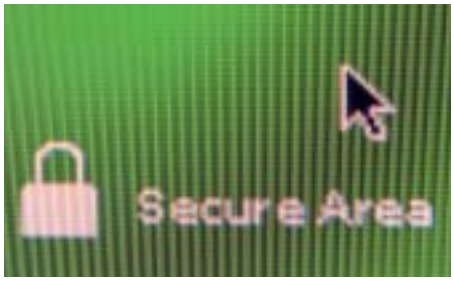
Prüfung von Linux und Unix

# Allzeit bereit mit der stets verfügbaren Sicherheitszone

In Zeiten knapper Kassen bieten sich Linux und Unix als vergleichsweise kostengünstige Serverbetriebssysteme an. Zudem genießen sie den Ruf, Verfügbarkeit in einem höheren Maße als Alternativen zu garantieren. Doch wie steht es mit der Sicherheit? Gerade wenn Server auch von „außen“ erreichbar sein müssen, rückt diese Frage in den Vordergrund. Sie sind also aufgerufen, hier dem § 9 BDSG mit der Kontrolle der technischen Maßnahmen Genüge zu tun.




Legen Sie bei der Prüfung von Linux Ihr Hauptaugenmerk auf die „schlanke Linie“ des Systems. Dann klappt's auch mit der Sicherheit.

Um einen Server sicher zu konfigurieren, sind einige Grundsätze zu beachten, die völlig losgelöst vom konkreten Betriebssystem sind. Wenn ein Programmierer Software schreibt, wird er Fehler machen. Dabei ist es egal, ob er Open-Source-Software (z.B. Linux) oder Closed-Source-Software (z.B. Windows) schreibt. Die Zahl der Fehler hängt auch vom Umfang des Quelltexts ab. Damit lässt sich die Zahl der Fehler reduzieren, wenn man den Umfang der Software reduziert.

## Die eingesetzte Software muss auf das Notwendigste beschränkt werden

Es sind also – bei gleicher Qualität der Programmierer bzw. der Tester – in einem Megabyte Software weniger Fehler – und damit potenzielle Sicherheitslücken – als in einem Gigabyte. Deshalb muss der Umfang der eingesetzten Software so gering wie möglich sein, um die Wahrscheinlichkeit für Sicherheitslücken zu reduzieren.

## Ein „Out of the Box“-Linux ist für einen Server absolut ungeeignet

Ein Linux, von der CD-ROM der Distribution frisch mit Default-Einstellungen installiert, enthält fast immer zu viel unnötige Software. Für einen Büroarbeitsplatz mag die Auswahl richtig sein, für einen Server ist sie zu umfangreich. Es gilt also, zu entschlacken – und zu überprüfen, ob das tatsächlich auch geschehen ist. Selbst der vom BSI zur Verfügung gestellte Behördendesktop ERPOSS3 orientiert sich mehr am Bedarf eines Entwickler als am Bedarf eines Sachbearbeiters (*www.bsi.de/produkte/erposs3*).

Eine Linux-Distribution, die auf den sicheren Einsatz als Server abzielt, ist Devil-Linux (*www.devil-linux.org*). Hier wird auf eine grafische Oberfläche ebenso verzichtet wie auf Entwicklungswerkzeuge. Trotzdem kann und sollte diese Distribution vor dem Produktiv-Einsatz noch optimiert werden. Dieses Linux kann als

- Router
- Firewall
- Proxy-Server
- DNS-Server
- Mail-Server mit TLS-Unterstützung, Spam- und Viren-Filter
- Web-Server
- FTP-Server
- File-Server

eingesetzt werden. Beim Einsatz als z.B. Firewall sollten dann alle anderen Server-Anwendungen entfernt werden.

### Wohin mit den Protokolldateien?

Jedes System sollte wichtige Ereignisse protokollieren, damit sich Vorfälle entdecken und analysieren lassen. Ein Einbruch in ein System, ohne Spuren in den Protokolldateien zu hinterlassen, ist unmöglich. Kontrollieren Sie deshalb, ob eine regelmäßige und zeitnahe Auswertung der Dateien stattfindet.

Ein Eindringling wird aber versuchen, seine Spuren in den Protokolldateien zu löschen, um seine Entdeckung zu erschweren. Die Protokolldateien müssen daher geschützt gespeichert werden.

Eine Möglichkeit ist, einen speziellen Log-Server zu verwenden. Alle Syslog-Varianten – syslog ist der de-facto-Standard zur Speicherung und Übermittlung von Protokollmeldungen in einem Rechnernetz – unterstützen dies.

## Patchen und das „andere“ Erforderlichkeitsprinzip

Sobald Sicherheitslücken in einer Software gefunden werden, gibt es eine korrigierte Version (Patch oder Sicherheitsupdate). Da spätestens mit der Veröffentlichung die Sicherheitslücke allgemein bekannt ist, drängt jetzt die Zeit, das Update auch einzuspielen. Zu einer sicheren Installation gehört deshalb immer ein aktueller Stand der installierten Updates. Auch dies spricht für einen möglichst geringen Umfang an installierter Software, da nicht installierte Software auch nicht aktualisiert werden muss.

## Je weniger Rechte verteilt werden, desto weniger können auch „feindlich übernommen“ werden

Auf jedem „vernünftigen“ Betriebssystem gibt es verschiedene Benutzer, die mit unterschiedlichen Rechten agieren. Der Administrator (unter Linux/Unix der Benutzer „root“) darf alles. Ein normales Programm benötigt zur

Nutzung aber im Allgemeinen nicht so umfassende Rechte. Deshalb können viele Programme auch unter reduzierten Rechten gestartet werden.

Ein Hacker, der über ein Programm (z.B. mittels eines Buffer Overflow) in das System einbricht, bekommt die Rechte des Programms. Je weniger Rechte das Programm hat, desto weniger Rechte hat der Hacker. Fragen Sie daher nach, ob das Programm entsprechend konfiguriert wurde.

### Hacker ein- statt aussperren

Mit dem Kommando chroot (change root) kann ein Unix- bzw. Linux-Befehl oder -Prozess in einem anderen Hauptverzeichnis gestartet werden. Damit wird diesem Prozess eine anders geartete Laufzeitumgebung vorgegaukelt. Der Prozess sieht nicht die originale Systemumgebung, sondern eine speziell präparierte mit anderen Konfigurationsdateien, anderen Passwortdateien etc. Soweit ein Hacker aus dieser „Falle“ nicht ausbrechen kann, kann er die Konfiguration des Systems nicht zerstören.

Mit dem Linux vserver oder dem BSD Jail wird das chroot-Konzept in Richtung auf virtuelle Server erweitert. So ist eine noch bessere Abschottung vom eigentlichen Betriebssystem möglich.

### Wer sich nie anmeldet, braucht auch kein Passwort

Jeder Benutzer, der sich am System anmelden will, benötigt ein Passwort. Benutzer, die sich nie anmelden, benötigen auch kein Passwort. Ein Passwort ist leicht zu deaktivieren. Dazu wird in der Datei /etc/passwd bzw. /etc/shadow einfach in das Password-Feld ein einzelnes Zeichen eingefügt. Damit ist sichergestellt, dass eine Passwortüberprüfung immer einen Fehler liefert.

Es ist auch möglich, für alle Benutzer das Passwort zu deaktivieren, wenn man sich darauf beschränken will, eine Anmeldung nur per SSH mit Authentifizierung per Schlüssel zuzulassen. Hierzu muss es aber eine Möglichkeit geben, den öffentlichen Schlüssel vor der ersten Anmeldung auf den Server zu bringen.

### Die Datenintegrität lässt sich durch Prüfsummen kontrollieren

Will man von Zeit zu Zeit die Integrität des Systems prüfen, empfiehlt es sich, Prüfsummen von allen wichtigen Dateien zu bilden. Gebräuchlich sind dazu einfache Tools wie „md5sum“ oder „sha1sum“ oder Spezialprogramme wie „tripwire“. Diese Programme berechnen Prüfsummen der Programmdateien, sodass durch einen Vergleich festgestellt werden kann, ob Dateien manipuliert wurden.

### Fahrlässig handelt, wer Prüfsummen lokal speichert

Hierzu sind aber zwei wichtige Bedingungen notwendig. Die berechneten Prüfsummen dürfen nicht auf dem entsprechenden Rechner gelagert werden. Gut geeignet ist eine Auslagerung auf eine CD-ROM. Außerdem muss der Rechner zur Überprüfung ein anderes Betriebssystem wie KNOPPIX oder BartPE booten, damit sichergestellt ist, dass kein Root-Kit das Ergebnis der Überprüfung verfälschen kann.

Es hat keinen Sinn, Dateien, die sich regelmäßig ändern, in die Prüfsummenbehandlung aufzunehmen. Außerdem muss der Datenträger mit den Prüfsummen nach jedem Programm-Update aktualisiert werden, da sich die Prüfsummen der aktualisierten Dateien geändert haben.

### Alles, was nicht nutzt, kann schaden!

Das Grundprinzip der Absicherung eines Rechners besteht im Abspecken. Prüfen Sie daher, ob alles, was nicht benötigt wird, entfernt wurde. Die Rechte müssen beschnitten, der Zugriff so weit möglich eingeschränkt sein. Dann kann ein Eindringling auch nur wenig anrichten.

Trotzdem muss ein System gepflegt werden, d.h. Updates und Korrekturen müssen ständig eingespielt werden. Die Protokolldateien werden regelmäßig inspiziert.

*Prof. Dr. Rainer W. Gerling*

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

#### Linux-Prüfung auf einen Blick

- Welche Software ist auf dem Rechner installiert?
- Welche Software wird davon wirklich benötigt?
- Ist ein Compiler auf dem Rechner installiert?
- Welche Benutzer sind angelegt?
- Welche Rechte haben diese Benutzer?
- Wie kann sich ein Benutzer am System anmelden?
- Welche Dienste laufen auf dem Rechner?
- Welche Dienste werden davon wirklich benötigt?
- Laufen die Dienste in einer sicheren Umgebung (reduzierte Rechte, Change-Root-Umgebung)?
- Wie werden Passwörter gespeichert?
- Wie ist das Betriebssystem konfiguriert (statischer oder modularer Kernel)?
- Sind alle Software-Pakete und das Betriebsystem auf einem aktuellen Stand?
- Sind alle verfügbaren Patches und Sicherheits-Updates eingespielt?
- Wo werden die Protokoll-Dateien gespeichert? In einer sicheren Umgebung?
- Gibt es Prüfsummen von allen statischen Dateien (Programmdateien, Konfigurationsdateien) auf einem externen, schreibgeschützten Datenträger?