

## Das Betriebssystem Linux

# Sicherheitsfunktionen für den Praxisbetrieb

In den letzten Jahren ist das Betriebssystem Linux immer mehr in Mode gekommen. Im folgenden Beitrag wird dargestellt, welche Stärken dieses Betriebssystem beim Schutz der Praxisdaten zu bieten hat.

Es ist aus drei Gründen notwendig, die Daten einer Arztpraxis zu schützen: Der Gesetzgeber regelt den Schutz der Patientendaten, der gesunde Eigennutz diktiert den Schutz der persönlichen und Geschäftsdaten (Abrechnungsdaten, Karteikarte), und die ärztliche Ethik gebietet den Schutz sensibler Daten ohnehin. Nach praktischen Gesichtspunkten teilt sich der Datenschutz in zwei große Bereiche: Schutz vor missbräuchlicher Verwendung und Schutz vor Verlust oder Verfälschung, das heißt, es geht um Geheimhaltung und Integrität der Daten. Beide Aspekte müssen unabhängig vom Computereinsatz in der Arztpraxis beachtet werden.

Im Folgenden wird die Geheimhaltung thematisiert; relevante Softwarepakete sind beispielhaft kursiv in Klammern aufgeführt. Auf eine Darstellung der Gefahren für die Integrität (Stromausfall, Brand, Hard- und Softwarefehler, Viren etc.) und möglicher Schutzmaßnahmen (Datensicherung, USV etc.) wird nicht eingegangen.

Ausgangsbeispiel ist eine Praxis mit Servern und vernetzten Arbeitsplätzen.

### Zugriffsschutz

■ **Identifikation berechtigter Nutzer:** Die Mitarbeiter der Praxis müssen sich bei Arbeitsbeginn beim Server und am Arbeitsplatzrechner als berechtigte Nutzer anmelden. Dies geschieht üblicherweise über die Kombination von Benutzernamen und Passwort. Unter Linux kann man bestimmen, welches Ver-

fahren zur Verschlüsselung der Passwörter verwendet wird (*login*). Die Passwörter selbst lassen sich in einer speziell gesicherten Datei ablegen, die nur von dazu berechtigten Programmen gelesen werden kann (*shadowpasswd*). Es lässt sich festlegen, welche Nutzer den Computer zu welchen Zeiten von wo aus benutzen dürfen. Um diese Beschränkungen durchzusetzen, können angemeldete Benutzer bei Beginn der Sperrzeit oder definierbar langer Inaktivität automatisch abgemeldet werden (*logout*). Alternativ kann die Sitzung eines inaktiven Nutzers mit passwortgeschützten Bildschirmschonern gesperrt



werden (*vlock*, *xautolock*). Maximale Gültigkeitsdauer und minimale Länge für Passwörter sind festlegbar. Verständlicherweise wählen Computeranwender gern einfache zu merkende und daher auch zu erratende Passwörter. Es gibt verschiedene Programme unter Linux (*john*), mit denen die Sicherheit vorhandener Passwörter getestet werden kann. Alternativen zur Passwordeingabe bieten biometrische Verfahren (Stimme, Gesicht, Fingerabdruck, Iris) oder Chipkarten. Für beide Varianten ist entsprechende Software für Linux in Arbeit.

Beim Anmelden am System werden berechtigte von unberechtigten Nutzern getrennt. Auf dieser Unterscheidung beruht der grundlegende Zugriffsschutz für Daten in einem Linuxsystem, der durch die seit Jahrzehnten bewährten Dateirechte geregelt wird. Die Nutzer eines Computers werden mit Blick auf

die Daten in drei Gruppen eingeteilt: Eigentümer der Daten, Angehörige der gleichen Nutzergruppe wie der Eigentümer, andere Nutzer bzw. Nutzergruppen. Für jeden Personenkreis können die Rechte „Lesen“, „Schreiben“ und „Ausführen“ individuell vergeben werden. Dadurch wird sichergestellt, dass nur berechnete Personen Informationen lesen, verändern und löschen können.

■ **Schutz bestimmter Einträge in der Karteikarte:** Innerhalb der Praxissoftware kann es notwendig sein, bestimmte Daten nur bestimmten Benutzern zugänglich zu machen. Die Unterscheidung, wer welche Informationen aus der elektronischen Karteikarte einsehen darf, übernimmt das Praxisprogramm, da dort festgelegt ist, welche Daten welche Bedeutung haben und eigens geschützt werden müssen. Das Betriebssystem kann daher nicht für den Schutz von Inhalten zuständig sein, sondern nur für die allgemeine Zugangsberechtigung zu Dateien. Linux bietet der Praxisanwendung verschiedene Mechanismen, die starke Grundsicherheit für die Nutzertrennung zu speziellen Zwecken zu nutzen (*PAM*, *capabilities im Kernel*). Dadurch wird es einem Anwender mit weniger Rechten erschwert, unberechtigt die Identität eines anderen Anwenders mit erweiterten Rechten anzunehmen.

■ **Physikalischer Schutz:** Bei fast jedem Betriebssystem gibt es im Hinblick auf den Dateizugriffsschutz das Problem, dass dieser nur wirksam ist, solange keine unberechtigte Person physikalisch Zugang zu dem geschützten Computer hat. Da der Zugriffsschutz nur funktioniert, wenn das Betriebssystem mit der nötigen Software geladen wurde, ist es möglich, den Schutz zu umgehen, indem man ein eigenes Betriebssystem von einer Bootdiskette/-CD oder einer anderen Festplatte startet. Man kann auch eine gestohlene oder be-

schlagnamte Festplatte in einen anderen Computer einbauen und die Daten kopieren. Daher gilt: „Es gibt keine Sicherheit ohne physikalische Sicherheit.“ Ein Computer mit Linux muss hier auf gleiche Weise geschützt werden wie jeder andere Computer, bietet aber mehrere Mechanismen an, die physikalische Sicherheit zu erhöhen:

- Passwortabfrage vor dem Booten (*lilo, grub*),
- Betrieb des Servers ohne Tastatur, Diskettenlaufwerk oder Monitor;
- Deaktivierung der Unterstützung von Disketten- oder CD-ROM-Laufwerken.

Linux bietet auch die Möglichkeit, das Herunterfahren und Neustarten des Computers nur bestimmten Nutzern zu erlauben. Dies ist aber nur vorteilhaft, wenn der Zugang zum Netzschalter, zum Resetknopf und zur Steckdose Unbefugten nicht möglich ist.

Allerdings lassen sich selbst solche Daten vor unberechtigtem Einblick schützen, die bereits in die Hände von Unbefugten gelangt sind: durch die Verschlüsselung der Daten auf der Festplatte. Hierzu gibt es die verschiedensten Pakete unter Linux, die bestimmte Dateien (*PGP, GPG*), das Heimatverzeichnis eines Anwenders (*BestCrypt*) oder ganze Partitionen (*ppdd, CFS*) verschlüsseln.

**■ Schutz im lokalen Netz der Praxis:**

In einem lokalen Netzwerk, wie es viele Arztpraxen heute nutzen, kann ein Angreifer mit geeigneter Software die zwischen Server und Arbeitsplatz ausgetauschten Daten belauschen. Dabei kann es sich um Patientendaten oder um Passwörter für den Zugriffsschutz handeln. Um dies zu vereiteln, bietet Linux verschiedene Verfahren wie SSL (Secure Socket Layer) und SSH (Secure SHell) an, die die Daten zur Übertragung ver- und entschlüsseln. Alternativ kann man das lokale Netz unter Linux mit der Version 6 des TCP/IP-Protokolls

(IPv6) betreiben, das bereits Verschlüsselungsmechanismen eingebaut hat (IPSec).

Schutz bei fortgeschrittenen Funktionen des Computersystems

**■ Nutzung eines Modems oder einer ISDN-Karte:** Modem oder ISDN-Karte werden häufig für folgende Zwecke eingesetzt:

- Wartung und Aktualisierung der Praxis-EDV per Fernwartung;
- Übertragen der Laborergebnisse vom Labor auf den Praxiscomputer;
- Einwahl von Kollegen in das Praxissystem zum Übertragen von Befundbriefen;
- Anbindung eines Arbeitsplatzes zu Hause oder in Zweigstellen per Telefonleitung.

Für diese Anwendungen bietet Linux verschiedene Sicherheitsmaßnahmen: Der Verbindungsaufbau kann durch Auswertung der Rufnummer des Anrufers (ISDN, einige Modems), verschlüsselte Abfrage von Zugangspasswörtern (Modemfunktion, *pppd* bzw. *ipppd* mit CHAP) oder Callback geschützt wer-

den (Zweigstelle, zu Hause) werden unter Linux durch ein „Virtuelles Privates Netz“ geschützt (*vpnd, FreeS/WAN*).

Viele Ärzte nutzen den Zugang zu ihrer Bank über T-Online oder das Internet. Linux kann diese Verbindungen durch Verschlüsselung schützen (SSL) und stellt zudem sicher, dass nur berechnete Benutzer Zugriff auf Bankprogramme, Kontodateien und Modem bzw. ISDN-Karte haben. Für Netscape gibt es eine Erweiterung (*fortify*), die sichere Verschlüsselung mit langen Schlüsseln ermöglicht. All diese Verfahren beruhen auf wohldefinierten, verbreiteten und erprobten Standards. Damit ist Linux auch für künftige telemedizinische Anwendungen gerüstet, wie die Übertragung von Befunden, das Einreichen der Abrechnungsdaten per Modem oder die netzgestützte elektronische Karteikarte.

**■ Sichere Nutzung des Internets:**

Aus einer modernen Praxis ist die Nutzung des Internets nicht mehr wegzudenken. Grundsätzlich wird empfohlen, das Praxiscomputersystem und den Rechner zum Surfen im Internet und für E-Mail zu trennen. Allerdings sind große Netze, wie zum Beispiel das DGN oder T-Online, nicht vollständig physikalisch vom Internet getrennt (sonst wäre kein Surfen über den DGN-Zugang möglich), sondern durch hochsicher konfigurierte Schutzrechner an den Übergangsstellen abgeschottet. Diese Sicherheit ist mit Linux oder OpenBSD ([www.openbsd.org](http://www.openbsd.org)) auch in der Arztpraxis möglich und bezahlbar.

Aus Stabilitäts-, Sicherheits- und Performancegründen sollte der Zugangsschutzrechner für das Internet vom Praxisdaten-Server getrennt werden. Linux bietet unterschiedliche Möglichkeiten, den Zugang von außen auf das Praxisnetz und von innen auf das Internet zu regulieren. Der Zugang selbst und einzelne Verbindungen zu bestimmten Servern (E-Mail, WWW, ...) können unter Linux mittels SSL, SSH oder *fortify* verschlüsselt werden. Eine Firewall lässt nur ausdrücklich erlaubte Pakete in das Internet hinaus beziehungsweise in das Praxisnetz hinein. Ein weiterer Türsteher (*tcp\_wrapper, tcpd, xinetd*) erlaubt nur



den. Eine Firewall (*ipchains*) sorgt dafür, dass nur zugelassene Datenpakete die Praxis verlassen können und unerwünschte

Gäste draußen bleiben müssen. Die Verbindung selbst kann mit den bereits erwähnten Verfahren SSL, SSH oder IPv6 verschlüsselt werden. Unabhängig von diesen Maßnahmen kann man unter Linux die zu übertragenden Daten selbst durch Verschlüsseln vor der Übertragung zusätzlich schützen (*PGP* und *GPG*, Letzteres von der Bundesregierung gefördert). Entfernte Arbeits-

bestimmten Nutzern den Zugang zu ausdrücklich genehmigten Diensten. Cache-Programme für WWW-Seiten (*squid*, *junkbuster*) können bestimmte Inhalte oder Adressen filtern. Monitorprogramme (*port\_sentry*) fahnden ständig nach bestimmten Aktivitätsmustern, die bei Einbruchversuchen aus dem Internet typischerweise erzeugt werden, oder überwachen wichtige Dateien auf Veränderungen (*tripwire*, *AIDE*). Selbst für das regelmäßige Sichten der Logdateien des Systems gibt es Software (*log-check*, *swatch*). All diese Pakete sind für Linux frei verfügbar.

In letzter Zeit sind Angriffe vom Typ „Denial-of-Service“ häufiger geworden. Hierbei wird ein Rechner im Internet mit Paketen überschüttet in der Absicht, dass dieser unter der Flut der Anfragen den Dienst quittiert. Linux bietet dagegen verschiedene Maßnahmen. Es können sämtliche Dienste – die tatsächlich notwendigen ausgenommen – gesperrt werden (*xinetd*, *tcpd*, *tcp\_wrapper*), eine Firewall (*ipchains*) verhindert das Annehmen von unerwünschten Paketen, und Monitorprogramme (*portsentry*, *scanlogd*) können solche Attacken erkennen, den Benutzer warnen und den Rechner automatisch davor schützen. Lokal lassen sich Limits für Ressourcen einstellen, beispielsweise wie viel Arbeitsspeicher oder Festplattenplatz ein Nutzer belegen darf.

■ **Sicherheit im Umgang mit E-Mail:** Verschiedene E-Mail-Programme für Linux (*pine*, *mutt*, *messenger*, *kmail*) unterstützen die Verschlüsselung per PGP oder GPG. Dadurch kann E-Mail mit persönlichen oder medizinischen Daten über das Internet technisch sicher übertragen werden. Per E-Mail kommt oft eine weitere Gefahr aus dem Internet. Es handelt sich um Computerviren und Trojaner. Erstere haben das Ziel, den betroffenen Rechner im Betrieb zu stören (zum Beispiel durch Absturz, Löschen von Dateien), während Letztere unberechtigten Personen Zugang zum Praxiscomputersystem verschaffen, sensible Daten ausspähen und versenden oder einen Virus einschleusen können. Linux ist im Gegensatz zu Windows nahezu vollständig immun gegen

diese Bedrohung, da die meisten dieser Schädlinge auf Ausnutzung von Lücken in Skriptsprachen (IRC, Visual Basic, Word, Excel) und der unsicheren engen Verzahnung von komplexen Programmen unter Windows beruhen. Zwar gibt es einige dieser Sprachen auch für Linux, aber ein Virus oder Trojaner ist auf-



Homepage des Linux-Distributors SuSE

grund der nutzerabhängigen Zugriffsrechte auf die Dateien des betroffenen Benutzers beschränkt und kann nicht das ganze Computersystem angreifen.

### Allgemeine Schutzmechanismen

Der größte Vorteil von Linux beim Datenschutz liegt darin, dass der Quellcode für die genannten Pakete und das Betriebssystem selbst frei verfügbar ist. Dadurch ist er einer ständigen kritischen Ansicht durch die Anwender ausgesetzt, so dass Sicherheitslücken schnell geschlossen werden können. Dies ist längst nicht bei allen populären Betriebssystemen Standard.

Nicht zu unterschätzen ist, dass bei Linux die Datensicherheit keine Kostenfrage darstellt, da für alle Schutzzwecke adäquate Software kostenneutral verfügbar ist. Die notwendige Dokumentation ist im WWW reichlich vorhanden (siehe [www.linuxsecurity.com](http://www.linuxsecurity.com), [www.securityportal.com](http://www.securityportal.com), [linuxtoday.com](http://linuxtoday.com)).

Eine weitere Stärke von Linux ist das Aufzeichnen sämtlicher relevanten Systemereignisse, das bis hin zum Aufzeichnen einzelner Aktionen der Benutzer gehen kann. Diese Protokollierung

lässt sich auch über ein Netz auf einen besonders geschützten Rechner umleiten und verschlüsseln.

Linux ermöglicht Anwendungsprogrammen, starke Verfahren zum weiterführenden Schutz ihrer Daten zu nutzen. Dazu zählen ACL (Access Control Lists), PAM (Pluggable Authentication Modules), einfache Listen von berechtigten/unberechtigten Nutzern und IP- oder MAC-basierte Zugriffsberechtigung. Weitere Technologien werden zurzeit auf Linux portiert, so die Nutzeridentifikation mit biometrischen Verfahren oder die CDSA (Common Data Security Architecture) von Intel.

Ein generelles Problem bei Unix-Systemen ist, dass der Systemadministrator sämtliche Rechte an allen Dateien und Diensten besitzt und somit keinerlei Beschränkungen unterliegt. Mit Linux kann man dieses Sicherheitsproblem entschärfen, indem man ein langes

Passwort für diesen Nutzer einrichtet und es in zwei Hälften teilt, die man zwei verschiedenen Vertrauenspersonen mitteilt. Zudem lässt sich für die Routinewartung ein spezieller Benutzername einrichten, der auf die Patientendaten keinen Zugriff hat. Dadurch ist immer das Einverständnis zweier Partner notwendig, wenn Arbeiten an den Dateien mit Patientendaten notwendig sind.

Die meisten Distributionen sind unmittelbar nach der Installation nicht so sicher eingerichtet, wie es möglich wäre (jedoch bei weitem sicherer als eine Installation von DOS oder Windows). Die Anbieter RedHAT (RedHAT Update Network) und Debian (*get-apt*) ermöglichen inzwischen das automatische Laden und Updaten von verbesserten Versionen der installierten Software. Zum Absichern eines Praxiscomputersystems unter Linux ist somit ein gewisser Arbeitsaufwand notwendig – wie bei jedem Betriebssystem. Zumindest jedoch bietet Linux für alle bekannten Sicherheitsprobleme Lösungen.

**Karsten Hilbert**

Weitere Informationen und Links sind unter <http://hilbert.webprovider.com> abrufbar. E-Mail-Adresse: [Karsten.Hilbert@gmx.net](mailto:Karsten.Hilbert@gmx.net)