So gelingt der Zugang zum Linux-System mit PAM, NIS & Kerberos, per Smartcard oder LDAP

Zeitgemäß authentifizieren

Die Nachfolger des altbekannten Passwortsystems glänzen mit deutlich höherer Sicherheit. Zeitgemäße Technologien wie Kerberos, PAM, LDAP und intelligente Chipkarten bereiten zudem den Weg zur netzwerkweit einheitlichen Authentifizierung. Achim Leitner

Inhalt

Um die Zugangsschranke eines Standard-Linux-Rechners zu passieren, genügt es, ein Passwort zu zücken. Doch Passwörter kann man ausspähen, zum Beispiel beim Eintippen am Rechner oder während der Übertragung im Netz. Der virtuelle Grenzwächter des Zielsystems hat keine Chance, einen Betrug zu bemerken, und lässt Eindringlinge mit gültigem Passwort durch.

Der schlechte Ruf dieses Systems hat seine Ursache auch in der Vergesslichkeit der User: Kaum jemand kann sich 20 Passwörter merken, die aus zufällig gewählten Zeichen bestehen und sich im Wochenrhythmus ändern. Sie greifen daher zum Naheliegenden und notieren ihre Geheimnisse, manchmal sogar auf gelbe Notizzettel, die am Monitor kleben. Statt seine Anwender zu mehr Disziplin und einem perfekten Gedächtnis zu zwingen, sollten sich Admins um einheitliche Kennungen für alle Dienste und bessere Authentifizierungsmechanismen kümmern.

Die moderne und sichere Technik sind Smartcards und Challenge-Response-Protokolle. Die Karte speichert die Zugangsdaten des Benutzers so sicher, dass niemand sie auslesen kann – auch nicht das Linux-System, an dem sich der User anmeldet. Über das kryptographische Protokoll kann die Karte beweisen, dass sie die geheimen Daten kennt. Wie das funktioniert und wie man Smartcard-Anwendungen selbst entwickelt, erklärt der Artikel ab Seite 50.

Scharfe Wachen

Wer eine reine Softwarelösung sucht, wird bei Kerberos fündig. Das etablierte Authentifizierungsprotokoll liegt inzwischen in Version 5 vor und sorgt sogar für Single-Sign-On: ein Mal authentifizieren genügt, per Krypto-Ticket gelingt der Zugang zu jedem weiteren Kerberos-fähigen Dienst. Kluge Admins profitieren von diesen Vorteilen, ohne ihre Netzwerk-Benutzerdatenbank zu wechseln. Sie kombinieren Kerberos mit NIS (Network Information Service). Der Artikel auf Seite 32 beschreibt, welche Schritte dazu nötig sind.

Viele Firmen setzen auf die Novell-Directory-Dienste. Spätestens seit Suse zu Novell gehört, sind die Produkte dieses Herstellers auch für Linux-Admins ein Thema. Sie müssen dazu nicht mal Novells Software auf ihren Linux-Client installieren: Der Verzeichnisdienst ist außer über die proprietären Schnittstellen auch per Standard-LDAP ansprechbar. Eine Schema-Erweiterung im E-Directory genügt. Ab Seite 46 beschreibt ein Artikel, wie diese Erweiterung aussieht und welche PAM- und NSS-Einstellungen unter Linux dazu passen.

Freie Wahl

Bei der Vielzahl an Authentifizierungsverfahren wäre es unzumutbar, wenn jede Applikation selbst alle Protokolle und Methoden implementieren müsste. Mit Pluggable Authentication Modules steht daher eine Standardschnittstelle zur Verfügung: Jedes Programm, das Benutzer authentifizieren will, bindet diese Bibliothek ein. Sie lädt dann zur Laufzeit das vom Admin gewünschte Modul und kümmert sich um die Details. Wie sich PAM konfigurieren lässt und wie Admins selbst Module dafür entwickeln, ist ab Seite 38 zu lesen. ■