

## Unix/Linux zentralisierte Access-Control-Systeme

### Situation

Viele Unternehmen betreiben Server-Farmen, welche auf Unix und/oder Linux basieren. Zentralisierte Benutzer- und Zugriffs-Management-Systeme für solche Systeme sind nicht einfach zu betreiben, da entsprechende Mechanismen in den Basis-Betriebssystemen weitgehend fehlen. Viele Unternehmen setzen deshalb auf generische Benutzer- und Rollen-Management-Systeme, sowie auf Systeme („Middleware“), welche die Verbreitung solcher Benutzer und Rollen auf Zielsysteme ermöglichen. Um einen sicheren Betrieb der Zielsysteme zu ermöglichen müssen entsprechende Rollen- und Rechte-Modelle erarbeitet und umgesetzt werden, von der abstrakten Definition bis hinunter zur Detail-Implementierung mit den technischen Mitteln des Betriebssystems.

### Cnlab AG-Dienstleistungen

Cnlab AG analysiert die abstrakten Rollen-Modelle, die Zuteilung der Rollen zu Benutzern, sowie alle involvierten Werkzeuge, welche schliesslich die Einstellungen für die technischen Berechtigungen in den Zielsystemen vornehmen. Das Ziel ist es, Schwachstellen zu identifizieren und potentielle Schäden, sowie die damit verbundenen Risiken zu identifizieren. Schliesslich werden Vorschläge für die Verbesserung der Situation aufgezeigt, wo solche notwendig erscheinen.

Die Methodik der Cnlab AG basiert auf unserer über 10 jährigen Erfahrung in verteilten Server-Systemen. Im Weiteren stützen wir uns auf etablierte Standards (ISO27002, BSI, OWASP, OSSTMM).

### Projekttablauf

Projekte starten mit einer Analyse-Phase des abstrakten Rollen-Modells und der Mechanismen, welche zur Bestimmung und Einstellung der technischen Benutzerberechtigung auf den Zielsystemen eingesetzt werden. Basierend auf der Analyse werden die kritischen Rollen identifiziert. Für die kritischen Rollen, werden die vergebenen Einstellungen der Zielsysteme im Detail analysiert (z.B. Root-Zugriffe, SU-Konfigurationen, Sudo-Konfigurationen). Abschliessend werden die allfällig notwendigen Anpassungen der Einstellungen für die Zielsysteme erarbeitet („hardening“).

Der Aufwand zur Durchführung entsprechender Projekte ist abhängig von der Komplexität, sowie der Grösse der Systeme, sowie vom gewünschten Detaillierungsgrad. Übliche Projekte beanspruchen 5 bis 20 und mehr Personentage.

### Success Stories

Unsere Erfahrungen basieren hauptsächlich auf grossen Server-Infrastrukturen von Schweizer Banken, welche unter anderem ausgewählte Aufgaben durch Personal im Ausland ausführen lassen. Basierend auf dem Schweizerischen Bankgeheimnis, sind spezielle Sicherheitsanforderungen notwendig. Beispielsweise muss sichergestellt sein, dass die Rollen und Rechte solcher Mitarbeiter nicht für den Zugriff auf sensitive Daten missbraucht werden können. Unsere Reviews haben gezeigt, dass Missbräuche möglich sind, falls nicht angemessene Sicherheitsvorkehrungen getroffen werden.

### Cnlab AG Kontakte

Detaillierte Informationen erhalten Sie von folgenden Cnlab AG-Mitarbeitern:

Thomas Lüthi                      Tel +41 55 214 33 41

Paul Schöbi                        Tel +41 55 214 33 33