Universität des Saarlandes – Fachbereich 14 - Informatik

Hinweise zur Systemsicherheit

[Stand: 21.4.1995]

Die Systemsicherheit erfordert, daß jeder Account im System so gut wie möglich gegen unberechtigte Benutzung geschützt wird. Jeder Benutzer muß sich dabei für die Sicherheit seines Accounts verantwortlich fühlen. Denn ist erst einmal ein Einbruch in einen schlecht gesicherten Account gelungen, können nicht nur die Systemressourcen im Namen dieses Benutzers mißbraucht werden, sondern es sind auch alle anderen Benutzer durch die neuen Möglichkeiten des Einbrechers bedroht.

Diese Checkliste soll dem Benutzer Hinweise geben, mit welchen Maßnahmen er zur Verbesserung der Systemsicherheit beitragen kann:

- erkannte Sicherheitsmängel dem Anlagenbetreiber melden und nicht ausnutzen
- Regeln für den Umgang mit Passworten beachten:
  - -- das Passwort soll 8 Zeichen lang sein
  - -- das Passwort soll kein Wort mit einer Bedeutung sein
  - -- das Passwort soll kein Wort aus einem Wörterbuch sein
  - -- das Passwort soll nicht aus persönlichen Daten hergeleitet sein
  - -- das Passwort soll nicht aus bekannten Abkürzungen gebildet werden
  - -- das Passwort soll Groß- und Kleinbuchstaben, Ziffern, Satzzeichen enthalten

  Beispiel:

  Wahl eines Satzes mit einer Bedeutung, den man sich merken kann. Der Reihe nach den ersten Buchstaben jedes Wortes und die Satzzeichen als Passwort nehmen.

  - -- das Passwort ist geheimzuhalten
  - -- das Passwort ist regelmäßig zu ändern (ca. alle 3 Monate)
  - -- auf verschiedenen Sicherheitsclustern* sind unterschiedliche Passworte zu wählen
  - -- keine Passworte im Klartext im Rechner (in Scripts, etc.) ablegen
- die Nutzung des eigenen Accounts auch keinem “guten Freund” erlauben
- nach Sitzungsende abmelden (ausloggen)
- auch bei kurzzeitiger Abwesenheit möglichst das Terminal sperren oder den Raum abschließen
- kein World-Write-Zugriff auf das Homedirectory und alle eigenen Files
- kein World-Zugriff auf Punkt-Files wie .login, .cshrc, .profile, usw.
- kein World-Exec-Zugriff auf eigene Programme (Risiko für den Aufrufer)
- World-Read-Zugriff auf eigene Files nur in Ausnahmefällen
- keine set-UID Programme mit World-Exec-Zugriff
- keine set-UID oder set-GID Scripts
- umask auf Wert 077 setzen
- eigene Dateien mittels “ls -alc” von Zeit zu Zeit auf Plausibilität (Name, Eigentümer, Zugriffsschutz, Datum) überprüfen
- nur sichere Directories in die Definition des Kommandosuchpfades (CSH-Variable path, SH-Variable PATH, Environment-Variable PATH) aufnehmen
- Current-Directory (“.”) als letztes Directory in PATH bzw. path eintragen
- kein “+” im .rhosts-File
- kein Rechner und User aus anderem Sicherheitscluster im .rhosts-File
- kein Eintrag ohne Userangabe im .rhosts-File
- keine “alten” Einträge (Hosts , User) im .rhosts-File
- in .netrc-File nur Einträge für Zugang zu anonymous FTP, keine Passworte
- Vorsicht bei der Ausführung von Programmen aus anderen User-Directories (unerwünschte Nebenwirkung, Trojanisches Pferd)
- kein Kommando “xhost +” oder “xhost +Rechnername” geben
- Passwort-Eingaben über xterm nur im Secure-Mode machen (Option Secure-Keyboard oder secureonpwd)

*) ein Sicherheitscluster bilden z.B. die Ausbildungsrechner oder die Anlagen eines Lehrstuhls.