

9 Systemsicherheit



- Generelle Überlegungen
- lokale Sicherheit
- Netzwerksicherheit

9.1 generelle Überlegungen



das 100% sichere System...

- steht in einem Tresor in irgendeinem Bunker,
- hat keine (Netz-)Verbindung nach aussen,
- nützt rein gar nichts.

9.1 generelle Überlegungen(2)



- Sicherheitskonzepte werden von Menschen erdacht und Menschen sind nicht unfehlbar
- viele Konzepte werden ausgehebelt durch...
 - Bequemlichkeit
 - Unaufmerksamkeit
 - Schlampigkeit
 - Zeitmangel / Kostengründe

9.2 lokale Sicherheit



- Schutz vor
 - “legitimen” Usern mit “bösen” Absichten.
 - Hacker die bereits Zugriff auf das System haben.
 - Menschen mit physikalischem Zugriff zum System.

9.2.1 Passwörter



- Benutzer sollten auch dann Passwörter verwenden, wenn sie meinen keine schützenswerten Daten zu haben.
- Passwörter sollten nicht trivial sein,
- nicht im Lexikon enthalten sein.
- Administration: `/etc/login.defs` enthält
 - Gültigkeitszeitraum
 - Länge
 - Prüfung

9.2.2 /etc/passwd



- enthält Informationen über die User des Systems
 - ID
 - GID
 - Login Shell
 - Homeverzeichnis
 - früher auch die Passworte
- muss world-readable sein, daher die Passworte in /etc/shadow

9.2.3 /etc/shadow



→ Beispieleintrag:

```
support:ddEXnC8xhBrly:12029:0:99999:7:::
```

```
User:verschlüsseltes Passwort:....
```

→ Details siehe man shadow

→ Verschlüsselung funktioniert nur in eine Richtung

9.2.4 Setuid & Verzeichnisse



- Keine Schreibberechtigung für normale Benutzer in Verzeichnissen wie `/etc`, `/bin` ..., denn
 - z.B. könnte ein Benutzer könnten dort Skripte ablegen, die aus Versehen von `root` ausgeführt werden, weil der Name einem gängigen Tippfehler entspricht. Ein solches Skript erstellt dann z.B. in `/tmp` eine Shell mit `setuid root`. So kann jeder ohne Passwort an eine `root shell` gelangen.
- Konsequenzen:
 - Der normale Benutzer sollte nur in seinem Homeverzeichnis und in `/tmp` Schreibberechtigung haben.
 - Die `PATH`-Variable des Benutzer `root` sollte möglichst restriktiv gesetzt sein.

9.2.5 Setuid & Mounten



→ Ein Wechselmedium darf aus demselben Grund nie setuid fähig gemountet werden, sonst erstellt sich ein Benutzer am heimischen PC eine CD oder eine Diskette mit einer Shell mit gesetztem setuid bit und erlangt wiederum ohne Passwort vollen Systemzugriff.

→ Konsequenzen:

Wenn schon dem Benutzer erlaubt sein soll, Wechselmedien zu mounten, so sollte darauf geachtet werden, dass für diese Bereiche keine Ausführungsrechte bestehen (Option "noexec" in /etc/fstab).

9.2.6 E-Mails & Attachments



- Binärdateien, die man als Attachment per E-Mail erhält oder aus dem Internet herunterlädt können beliebigen Code enthalten und sollten grundsätzlich nicht ausgeführt werden.
- Auch E-Mails selber können je nach verwendetem Mail-Programm und dessen Sicherheitseinstellungen ausführbaren Code enthalten, also vorsicht.
- Konsequenzen:
 - E-Mails lesen als Benutzer root sollte nicht zur Gewohnheit werden, besser einen "normalen" Benutzeraccount anlegen und die Mails von root dorthin weiterleiten.

9.2.7 Browser



- Für Webbrowser gilt dasselbe wie für Mailprogramme, nur noch extremer.
- Jede Webseite kann Programmcode enthalten, der eine Sicherheitslücke des Browsers ausnutzt, um das System zu manipulieren.
- Selbst wenn man die einschlägigen Regeln (JavaScript abschalten, usw.) beachtet, ist man
 - frustriert, weil die Hälfte der Webseiten nicht funktionieren,
 - trotzdem nicht 100% sicher.
- Konsequenzen:
 - Unter der root id laufende Webbrowser sollten absolut tabu sein.

9.2.8 physikalischer Zugriff



- wer physikalischen Zugriff auf einen Rechner hat ist eigentlich auch schon root.
- jedes wichtige System unter Verschluss halten, bzw. nur solchen Menschen zugänglich machen, denen man 100%ig trauen kann.
- daher ist alles, was man für ein System tun kann, welches öffentlich zugänglich ist, es potentiellen Hackern so schwer wie möglich machen:
 - booten von Diskette, CD usw. nicht erlauben,
 - das BIOS mit einem Passwort schützen,
 - den Bootmanager mit einem Passwort schützen.
 - wenn möglich, Gehäuse abschliessen,
 - und nicht zuletzt den Rechner anketten.

9.2.9 Updates



- Jede auf einem System installierte Software kann Fehler enthalten, die sich als potentielle Sicherheitslücken erweisen.
- Fehler werden ständig gefunden und es ist nur eine Frage der Zeit, bis ein solcher ausgenutzt wird bevor er behoben ist.
- Konsequenzen:
 - die auf einem System installierte Software sollte immer auf dem aktuellsten Stand sein
 - Nicht benötigte Software sollte nicht nur nicht laufen, sondern gar nicht erst installiert sein, denn Programme aktuell zu halten, die nicht benötigt werden ist Zeitverschwendung.