Security & Firewalls: schneller Sicherheits-Check

Alltägliche Frage:

"Können Sie bitte meinen Server durchchecken?"

Meine übliche Antwort:

"Ja, aber was erhoffen Sie sich davon, oder wonach soll ich speziell suchen?"

Die meist unqualifizierte Antwort des (noch) potenziellen Kunden:

"Naja, nach Sicherheitslücken, nötigen Updates, Firewall und so..."

Übliche Vorgehensweise:

Einloggen, Anzahl der Server-Reboots überprüfen, Syslog/Messages grob checken, Speicher- und Prozessauslastung anschauen, einen Blick in die PHPinfo werfen und einige Scripte laufen lassen.

Das Geheimnis daran ist natürlich, die Daten auswerten zu können und die entsprechenden Maßnahmen einzuleiten oder den Kunden über die anstehenden Probleme aufzuklären.

Dabei helfen in der Regel folgende Scripte:

- Rootkit Hunter und/oder chkrootkit
- Lynis
- und ein eigenes Script

Dabei ist immer wichtig die aktuellsten Versionen zu nutzen.

ChkRootkit

ChkRootkit muß immer erstmal kompiliert werden:

```
cd /usr/local/src
wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
tar xzf chkrootkit.tar.gz
```

```
cd chkrootkit*
make sense

#starten
./chkrootkit
```

Rootkit Hunter

Einfach runterladen, auspacken, aufrufen:

```
cd /usr/local/src
wget http://heanet.dl.sourceforge.net/sourceforge/rkhunter/rkhunter-1.3.2.tar.gz
tar xzf rkhunter-1.3.2.tar.gz
cd rkhunter-1.3.2
./installer

#starten
rkhunter --check
```

Lynis

Lynis kommt aus dem selben Haus wie Rootkit Hunter.

```
cd /usr/local/src/
wget http://www.rootkit.nl/files/lynis-1.1.8.tar.gz
tar xzf lynis-1.1.8.tar.gz
cd lynis-1.1.8

#starten (interaktiv):
./lynis --checkall

#starten (Volldurchlauf):
./lynis --checkall --cronjob --no-colors
```

Eindeutige ID: #1325
huschi
2008-08-04 23:51