Linux Server absichern

Ein Cheat- und Link-Sheet

Version 1.0, 01.03.2018, (c) Thomas-Krenn.AG, https://thomas-krenn.com/de/wiki

Sichere OpenSSH Konfiguration

```
Public Key Authentifizierung
   $ ssh-keygen -b 4096
   Mit Passphrase schützen
   Pubkey z. Server übertragen
   PasswordAuthentication no

SSH Root Login verbieten
   $ sudo sshd -T |grep -i permitrootlogin
   PermitRootLogin no

Login mit Fail2ban absichern
   cp /etc/fail2ban/jail.conf \
   /etc/fail2ban/jail.local
   Eintrag für SSH-Server setzen

2-Faktor-Authentifizierung per PAM Modul
   Public Key und One-Time-Password
   Installation: $ sudo apt install \
   libpam-google-authenticator
   Initialisierung: $ google-authenticator
   SSH Konfiguration anpassen:
   $ sudo vi /etc/pam.d/sshd
   $ sudo vi /etc/ssh/sshd_config
   $ sudo systemctl restart sshd.service
```

Wiki Artikel "Absicherung eines Debian Servers"

TKmag Artikel "Linux-basierte Root-server absichern"

iptables

```
Userspace-Programm zur Konfiguration
der Linux-Kernel Firewall
Dauerhafte Speicherung der Regeln
   $ sudo apt install iptables-persistent
Übertragung nach rules.v4 und rules.v6
   $ iptables-save > /etc/iptables/rules.v4
   $ iptables-save > /etc/iptables/rules.v6
```

Update-Management

```
Automatische Benachrichtigung bei Updates
   $ sudo apt install apticron
Autmatische Installation von Updates
   $ sudo apt install unattended-upgrades
   Konfiguration in /etc/apt/apt.conf.d/
```

Kein Backup, kein Mitleid

```
Zuverlässige Backup-Strategie
essentiell
Verschiedene Möglichkeiten:
   rdiff-backup, rsnapshot,
   rsync
```

TCP Wrapper

```
Zwischenschicht vor inetd, sshd, ...
Dienst muss libwrap unterstützen
   $ sudo apt install tcpd
/etc/hosts.deny
   ALL:ALL
   Per Wildcard alles verbieten
/etc/hosts.allow
   Einzelne IPs, Adressbereiche
   Selektiv erlauben
```

Sicherheitswerkzeuge

```
nmap: Scannen nach offenen Ports
   $ man nmap
   $ sudo nmap <IP-Adresse>
debsums: MD5-Summen installierter Pakete
   $ sudo apt install debsums
etckeeper: Protokollierung und Versionierung
von /etc/
   $ sudo apt install etckeeper
rkhunter, chkrootkit
   Aufspüren von Rootkits
logcheck: Auffälligkeiten in den Logs finden
   $ sudo apt install logcheck
lynis: Open Source Auditing-Tool
   Autom. Analyse mit Berichtsfunktion
Intrusion Detection Systeme
   tripwire, OSSEC (Host-basierte IDS)
   Alarmierung bei Veränderungen der Dateien
VPN-Zugang
   Statt Ports in der Firewall zu öffnen
   OpenVPN mit Zertifikaten verwenden
```

Sicherheitshinweis

Bei Konfigurationsänderungen,
zum Beispiel am SSH Daemon,
immer mit einer zweiten SSH Sitzung testen
und die bestehende Sitzung nicht schließen.

Dokumentation

```
$ sudo apt install man-db
man <Programm>
man ssh|sshd
man fail2ban
man iptables
```

THOMAS KRENN®