



# Securing Tru64 UNIX®

Reinhard Stadler  
HP Services

© 2004 Hewlett-Packard Development Company, L.P.  
The information contained herein is subject to change without notice



## Agenda

- Bedrohungen und Maßnahmen
- Security Features von Tru64 UNIX
- Installation und Konfiguration
- Welche Dienste sind notwendig, welche sind unwichtig
- Monitoring





## Computersicherheit

- Abwägung zwischen Benutzerfreundlichkeit und Sicherheit
- Abhängig von der Art des Systems
- Abhängig von der Sensibilität der Daten
- Abhängig von gesetzlichen Bestimmungen

May 23, 2006

3



## Bedrohungen

- Angriffe auf bestimmte Server Dienste durch
  - Buffer Overflows
  - DoS (Denial of Service)
- Angriffe auf Passwörter
  - Password-Sniffer
  - Social Engineering / Phishing
  - Passwörter „hacken“ oder standard Passwörter
- Angriff auf übertragene Daten

May 23, 2006

4



## Vorkehrungen

- technische Maßnahmen
- organisatorische Maßnahmen:
  - Notfallpläne bei Angriffen
  - Vorgaben zur Konfiguration
  - Kontrolle von Anwendern
  - Patch Policy
  - Untersuchung und Bewertung von Risiken und Schwachstellen
  - Monitoring

May 23, 2006

5

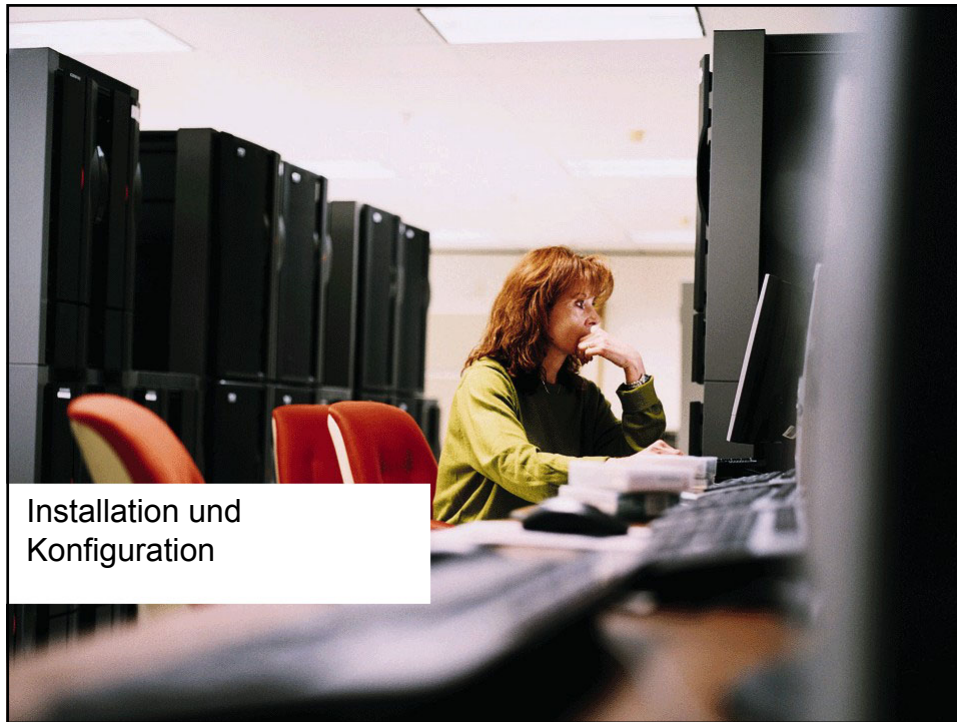


## Tru64 UNIX Security Features

- „Enhanced Security“
- SIA (Security Integration Architecture)
- leistungsfähiges audit tool
- IPsec
- SSH Secure Shell
- Single sign-on
- Single Security Domain im TruCluster

May 23, 2006

6



## Installation: Vorgehensweise

- Betriebssystem
- Patches
  - <http://itrc.hp.com>
  - <http://h30097.www3.hp.com/unix/security-download.html>
- Applications und Tools
- Absichern der Konfiguration
- Festschreiben
- Backup
- Sicheres Verwahren der Backups und Checksums



## Tru64 UNIX Secure Installation (1)

- eigenes Netzwerk für die Installation
- sichern der Hardware
  - Zugang zum Rechnerraum
  - Passwort auf F/W Ebene
  - Secure console mode
- Nur die benötigten Subsets installieren

May 23, 2006

9



## Tru64 UNIX Secure Installation (2)

- enhanced security subsets
- audit subset installiert und im kernel
- kdebug im kernel ist ein Schwachpunkt
- File System Layout:  
Filesysteme, in die alle schreiben können auf einer separaten Disk / Partition
  - /tmp
  - /var

May 23, 2006

10



## „Verriegeln“ des Systems

- enhanced security konfigurieren
- nützliche tools und utilities installieren
- Netzwerk Parameter anpassen
- unnötige Services abschalten
- nicht benötigte daemons abschalten
- Konfiguration der benötigten Dienste überprüfen
- auditing

May 23, 2006

11



## Enhanced Security Configuration

- ```
# sysman secconfig
```
- Enhanced Security
  - defaults for break-in detection
  - Execute bit set only by root
  - ACLs wenn benötigt
- 
- Default Templates anpassen
  
  - root account anpassen

May 23, 2006

12



## Nützliche Tools

- Open Source CD
  - <http://h30097.www3.hp.com/affinity/download.html>
    - `lsof`  
offene Ports und zugehörige Prozesse
- Internet Express Software Collection CD
  - <http://h30097.www3.hp.com/internet/osis.htm>
    - FireScreen (simple firewall based on screend)
    - `tcp_wrappers` - net services control

May 23, 2006

13

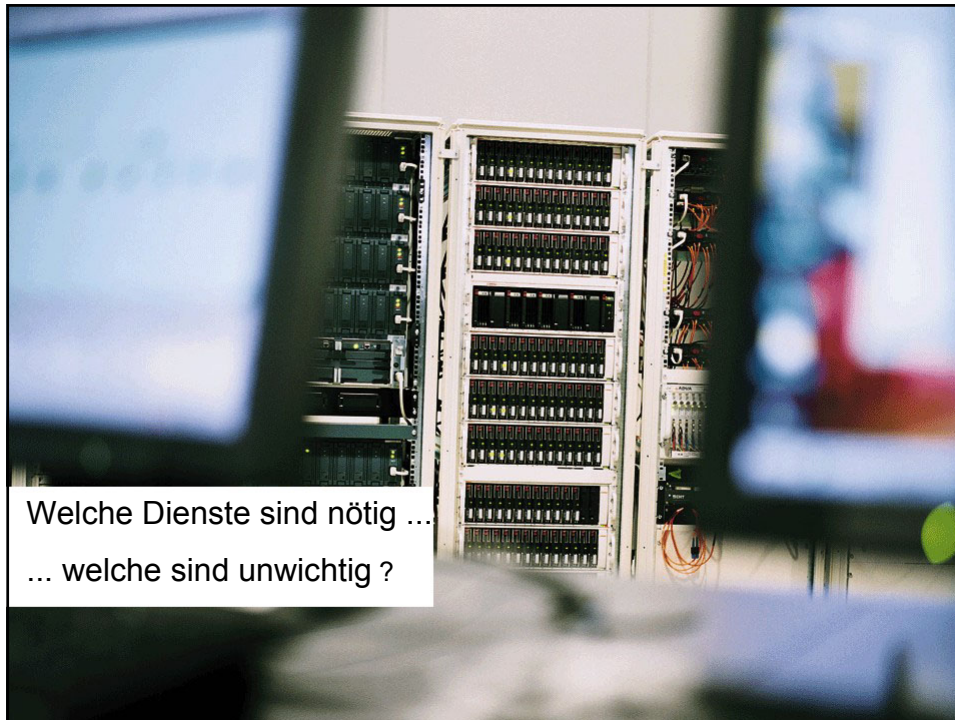


## Netzwerk Parameter

- `sysconfig -q socket`
  - `somaxconn`
  - `sominconn = somaxconn`
- `sysconfig -q inet`
  - `tcp_keepinit`
  - `icmp_tcpseqcheck`
  - `icmp_rejectcodemask`

May 23, 2006

14



## Network Services: /etc/inetd.conf (1)

- disabled by default
  - uucpd
  - fingerd
  - tftpd
  - talkd
  - bootpd
  
  - inetd internal services, tcp and udp versions  
daytime, echo, discard, chargen
  
  - RPC rstatd, rusersd, sprayd, walld



## Network Services: /etc/inetd.conf (2)

- Auf jeden Fall abzuschalten
  - comsat            - biff email notification
  - ntalkd            - talk server
  - Time internal service
  - kdebugd          - remote kernel debugger
  - rquotad          - quotas for remote file systems

May 23, 2006

17



## Network Services: /etc/inetd.conf (3)

- Wenn SSH genutzt wird:
  - rshd, rlogind
  - ftpd
  - telnetd
- Wenn das System kein Mailserver ist:
  - pop3
  - imapd
- Für Systeme, die nicht im Cluster sind:
  - cfgmgr            - für sysconfig -h .. -c ...

May 23, 2006

18



## Network Services: /etc/inetd.conf (4)

- **sysman Web Browser Interface:**
  - `suitjd` - Sysman suitlet java daemon
- **LSM GUI:**
  - `initlmsad` - LSM storage admin
- **Ohne X oder CDE:**
  - `dtspc`, - CDE subprocess control
  - `rpc.ttdbserverd` - RPC-based tooltalk db server
  - `rpc.cmsd` - calendar manager

May 23, 2006

19



## daemons (1)

- Über `rc.config` Variable, wenn diese im Startup Script abgefragt wird:
  - # `rcmgr set INSIGHTD_CONF NO`
- Umbenennen von Scripts:
  - `/sbin/rc3.d/S*`
    - `snmpd`
    - `smsd` - Sysman Station
    - `smauthd` - Sysman authentication
    - `lpd` - Line printer daemon
    - `advfsd` - AdvFS GUI

May 23, 2006

20



## daemons (2)

- Auf keinen Fall abgeschaltet werden dürfen:
  - evmd      Event Manager daemon
  - esmd      Essential Services Monitor daemon
  - caad      Cluster
- inetd kann abgeschaltet werden:
  - wenn SSH genutzt wird
  - das System nicht im Cluster ist
  - die Services, die inetd startet nicht genutzt werden

May 23, 2006

21



## daemons (3)

- Zeitsynchronisation  
xntpd oder ntpdate als cron job
- Sendmail
  - sendmail startup verhindern:  
/sbin/rc3.d/S40sendmail
  - Konfiguration:  
# sysman mail
  - Restrict to send-only

May 23, 2006

22



## was kann man sonst noch tun ... (1)

- Zugriff auf syslogd und binlogd

```
# touch /etc/syslog.auth (root, 600)
# touch /etc/binlog.auth
```
- Ausführen von cron Jobs:

```
# echo root >
/usr/lib/cron/cron.allow
# echo root > /usr/lib/cron/at.allow
```
- SNMP
  - ganz abschalten
  - Zugriff einschränken `/etc/snmp.conf`

May 23, 2006

23



## was kann man sonst noch tun ... (2)

- `/etc/ifaccess.conf` , `/etc/ftpusers` ,  
`/etc/securetty` ...
- Netzwerk Prozesse:

```
in /sbin/init.d/inetd
ulimit -c 0
```
- Zum Schreiben offene Verzeichnisse auf eine eigene Disk legen

```
/tmp, /usr/tmp, /var/tmp, ...
```

May 23, 2006

24



## sysconfigtab Parameter

- Executable stack (no = 0 = default)  
`# sysconfig -q proc executable_stack`
- Core Dumps (yes = 1 = default)  
`# sysconfig -q proc dump_cores`
- `setuid/setgid` um Core Dumps zu schreiben (no = 0 = default)  
`# sysconfig -q proc dump_setugid_cores`

May 23, 2006

25



## Audit

- Überwachen von Directories, wer Files anlegt, löscht, ...  
`# auditmask -x directoryname`
- Auditing einrichten:  
`# sysman auditconfig`
  - “networked\_system” event profile
  - “If log space exhausted, halt system” nicht auswählen
- Audit hilft nur, wenn die Logs überwacht werden!  
`# audit_tool ...`

May 23, 2006

26

## Agenda

- Bedrohungen und Maßnahmen
- Security Features von Tru64 UNIX
- Installation und Konfiguration
- Welche Dienste sind notwendig, welche sind unwichtig
- Monitoring



Fragen ?



