R|R|Z|N

Sicherheit
von
Servern
(Linux)

Serversicherheit - 2

R|R|Z|N

Vorbemerkung....3
Begriffsbestimmung....4
Begriffsbestimmung II/II....5
worüber ich nichts erzählen möchte....6
Grundprinzipien....7
Grundprinzipien II/II....8
Betrieb....12
Virtuelle Server....13
Überprüfung....15
Datensicherheit....16
Sonstiges....17

R|R|Z|N

Vorbemerkung

Dies ist eine Mischung aus Allgemeinem und ziemlich speziellen Beispielen.

Zum praktischen Vorgehen gibt es sehr viele Bücher und Kochrezepte, die man genau dann lesen sollte, wenn man sie benötigt.

Linux-Sicherheit: http://www.rrzn.uni-hannover.de/sicherheit.html

BSI-Empfehlungen für WWW-Server:
http://www.rrzn.uni-hannover.de/server_sicherheit.html

Begriffsbestimmung

Server
- Gegensatz: Client oder persönliche Workstation
- stellt irgendeinen Dienst zur Verfügung
- innere/äußere Dienste samba/www

Sicherheit
- Schutz ist Schutz der Daten oder Datenschutz
- Integrität der Daten
- Verfügbarkeit des Dienstes
- Hygiene – Daten bereinigen
- Authentizität – z.B. der Benutzer ist tatsächlich der, der er zu sein vorgibt
- Autorisierung – z.B. der Benutzer darf zugreifen

R|R|Z|N

Begriffsbestimmung II/II

Schlüssel
- symmetrisch – ein Schlüssel
- asymmetrisch – zwei symmetrisch verwendbare Schüsselhälften
- Zertifizierung – eindeutige Festlegung, zu wem ein Schlüssel gehört
- Server-Schlüssel – Schlüssel zum Rechner, nicht zum Dienst

DMZ – Demilitarisierte Zone ->Bild 1, 2; c't 2005/4-8

R|R|Z|N

worüber ich nichts erzählen möchte

- Menschliches
  - Arroganz/Ignoranz
    - uns passiert nichts
    - wir koennen das
    - Angreifer schaffen es sowieso nicht
    - wir sind hinter einem Firewall
  - Hacker/Cracker
    - aus Spaß/für die Mafia
- Passwörter
- Zugriffsrechte
- Aufstellungsort
- BIOS
- USV

R|R|Z|N

Grundprinzipien I/II

Minimalinstallation+Dienst+Schutz+Updates+Kontrolle

Minimalinstallation
- Basissystem
- kein X
- Editor
- ssh (Dämon) aus gesundheitlichen Gründen
  - kein root-Zugriff über ssh, d.h. nur 1 User und root
  - /etc/ssh/sshd_config: #PermitRootLogin yes => PermitRootLogin no
- Serverzertifikat

Dienst
- z.B. www oder ftp oder Samba oder Mail

R|R|Z|N

Grundprinzipien II/II

Schutz
- Firewall (extern oder lokal), z.B. iptables
- tcp-Wrapper – inetd, xinetd

Sicherheits-Updates
- SuSE: you, online_update
  - ftp://ftp.rrzn.uni-hannover.de/pub/mirror/linux/suse
- Debian: apt-get update
- Redhat: rpm -Fvh *.rpm oder yum update

Kontrolle
- syslog – Protokollierung des Vorgefallenen -> WOM
- tripwire – Unversehrtheit von Daten
- scanlog – Scan-Versuche bedeuten Gefahr
- logrotate – Kontrolliert die System-Logs, wirft alte weg („Hygiene“)
- cfengine – Kontrolle über alle Rechner im Netz

R|R|Z|N

tcp-Wrapper

inetd/xinetd kontrollieren Dienste/Ports

/etc/inetd.conf oder /etc/xinetd.conf+xinetd.d, services, hosts.allow, hosts.deny

froriep@anwserv1:~> cat **/etc/hosts.deny**
See tcpd(8) and hosts_access(5) for a description.
ALL: ALL EXCEPT LOCAL 130.75.
http-rman : ALL EXCEPT LOCAL

froriep@anwserv1:~> cat **/etc/hosts.allow**
See tcpd(8) and hosts_access(5) for a description.
sshd : ALL : ALLOW

R|R|Z|N

scanlog

Dämon, der überwacht, ob Portscans durchgeführt werden. Wenn ja, wird das in /var/log/messages vermerkt. Abfragebeispiel s.u..

R|R|Z|N

cfengine

Überwachung und Korrektur von Rechnern im Netz

Netzwerkeinbindung
Edieren von Textdateien (z.B. „trage ein, falls noch nicht vorhanden“)
Überwachung von Dateien, symbolischen Links, Zugriffs-, Eigentumsrechte
Verteilen von Dateien über das Netz, Korrekturen und Patches
Ausführen von Scripten
Prozessverwaltung

Bestandteile: cfagent, cfrun, cfservd, cfexecd, cfkey

cfenvd: Erkennung von Anomalien (Rechner verhält sich anders als normalerweise)

R|R|Z|N

Betrieb

überwacht

automatisiert (cron, /etc/cron.daily, weekly, monthly) siehe Beispiele unten

meldung per email, automatischer Vergleich

was passiert nach Stromausfall etc?

nicht automatisch:

- ssh - Aufschalten
- yast – Verwaltung (bei SuSE)
- webmin – Verwaltung über WWW
- Benutzerverwaltung Gruppen/Zugriffsrechte

R|R|Z|N

Virtuelle Server

chroot – Ändern der Dateisystemwurzel
uml – User Mode Linux (Beispiel c't-CD 2004/4 Vorsicht!!)
xen – Virtuelle Gastsysteme
vserver – Virtuelle Server
vmware - kommerziell

R|R|Z|N

vmware

Emulation eines PCs
- Hardware
- Bios
- Partitionierung

Linux/Windows/Solaris
Desaster Recovery
Netzanbindung über NAT oder Bridge
Testmöglichkeit durch virtuelles Netz aus virtuellen Rechnern

R|R|Z|N

Überprüfung

tcpdump, ethereal, snort, nmap, nessus

Beispiel Nessus www.nessus.org

nessus_installer.sh braucht noch gtk-devel openssl-devel

Congratulations ! Nessus is now installed on this host

. Create a nessusd certificate using /usr/local/sbin/nessus-mkcert
. Add a nessusd user use /usr/local/sbin/nessus-adduser
. Start the Nessus daemon (nessusd) use /usr/local/sbin/nessusd -D
. Start the Nessus client (nessus) use /usr/local/bin/nessus
. To uninstall Nessus, use /usr/local/sbin/uninstall-nessus

---

nessus-mkcert, nessus-adduser: trap: usage->(trap 0->trap – 0) <-bash version 3

R|R|Z|N

Datensicherheit

RAID5, hotswap, spare-Disc

Trennung von System- und Nutzdaten (usr/var)

Backup lokal, schnell Restore
- tar czf /backup/....tgz, (sh. Unten /etc/cron.daily/backup)
- dd if=/dev/hda1 | gzip -c >/backup/.... (vorher Partition putzen mit dd if=/dev/zero ...)

Netbackup
- Treiberinstallation (RRZN, Otto/Rode)
- Loch in Firewall
- Backup automatisch
- Restore mit x(bp)

Sonstiges

iptables: 3 Beispiele: nanni, suse, dummy (s.u.)

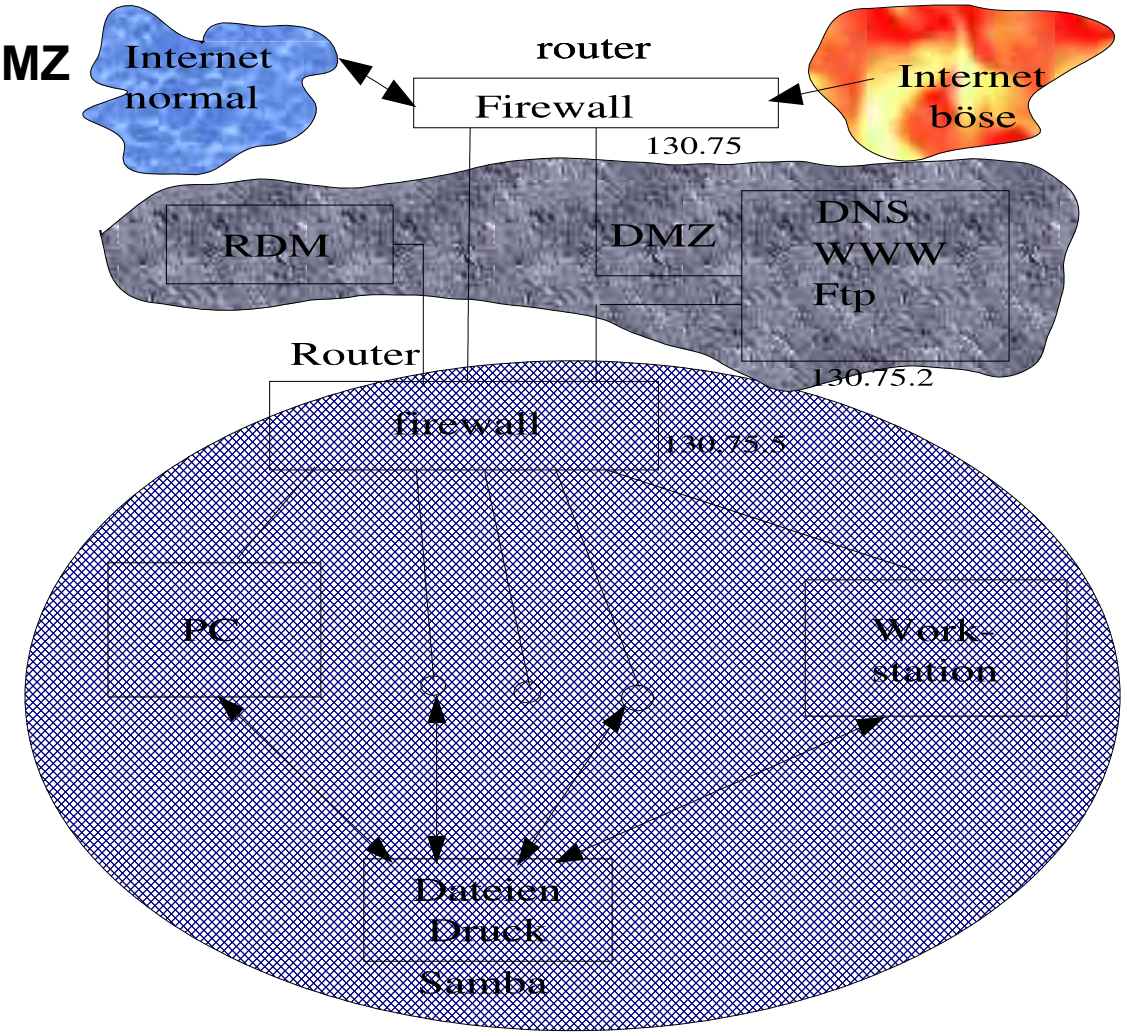
kontrolle@home

vpn/ipsec

cfengine+netz

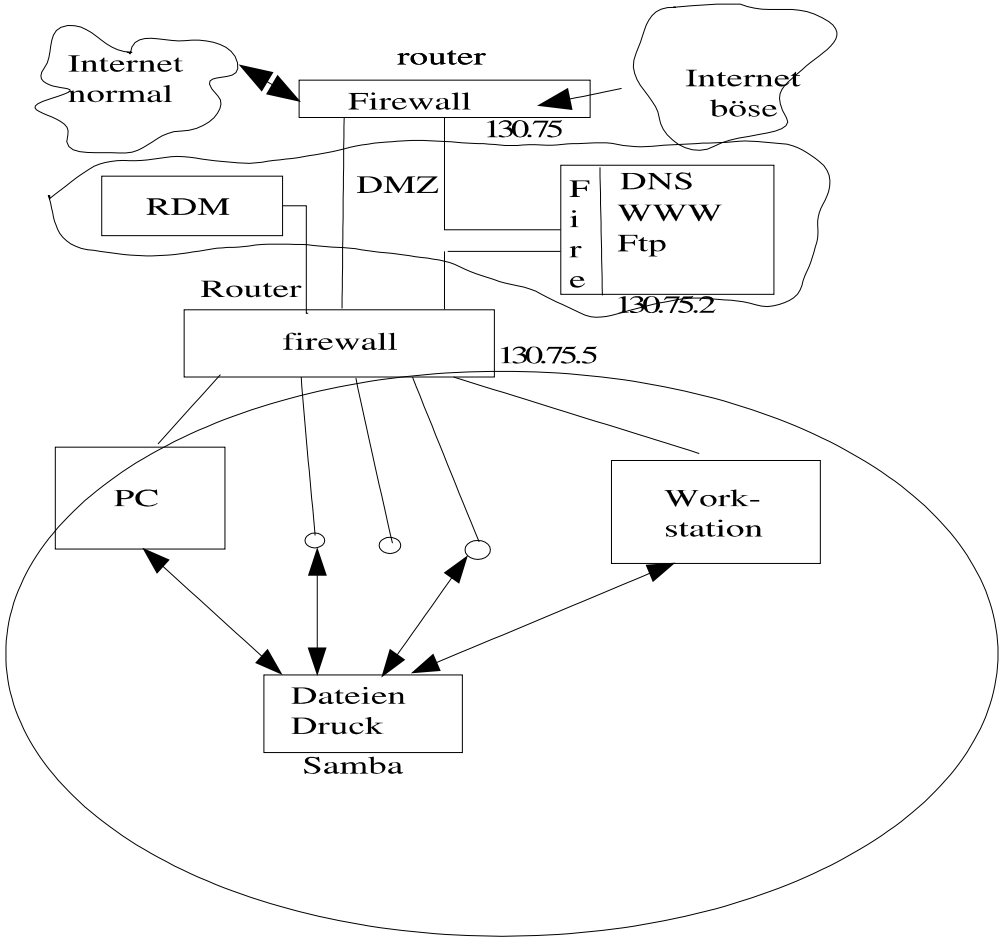
R|R|Z|N

Bild 1 DMZ



R|R|Z|N

Bild 2 DMZ



R|R|Z|N

Bild 3 – iptables

```
iptables -F INPUT                       # Alles leeren
iptables -F OUTPUT
iptables -F FORWARD
#
iptables -P INPUT DROP                  # alles schliessen
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
#
iptables -P OUTPUT ACCEPT               # von drinnen nach draussen
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
#
iptables -A INPUT -p udp  -s 130.75.1.40 --dport 123 -j ACCEPT     # Datum/Zeit
#
iptables -A INPUT -p tcp --syn --dport smtp -j ACCEPT              # Mail
#
iptables -A INPUT -p tcp --syn -s 130.75.0.0/16 --dport 22 -j ACCEPT # ssh eingeschr.
#
iptables -A INPUT -p tcp --syn --dport 80 -j ACCEPT         # apache von ueberall
iptables -A INPUT -p tcp --syn --dport 443 -j ACCEPT
#
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT       # ping
iptables -A INPUT -j LOG                                           # Logs
```

R|R|Z|N

Bild 4 cfengine.conf

```
control:
       domain = ( rrzn.uni-hannover.de )
       access = ( froriep root )
       actionsequence = ( links  tidy disable editfiles shellcommands )
       maxage = ( 7 )
groups:
       haveNoBin = ( pc1 pc2 )
tidy:
       /tmp pattern=* age=$(maxage) recurse=inf
       /home pattern=*~ recurse=inf
links:
       /logs -> /var/log
    HaveNoBin::
       /bin -> /usr/bin
disable:
       /var/log/httpd/access_log  rotate=2 size=>32kb
editfiles:
       { /etc/crontab  # cfengine in crontab
              AppendIfNoSuchLine "0 * * * * root /opt/local/bin/run-cfengine"}
shellcommands:
       haveNoBin.Hr12::
              "/usr/sbin/sendmail -q"
              "/usr/sbin/ntpdate 130.75.1.40 >/dev/null 2>/dev/null"
```

R|R|Z|N

Shellprozeduren zur Überwachung

/etc/cron.hourly/ntpdate
cron.daily/backup, logrotate, online_update, rogator, scanlog
cron.weekly/disktest

---

ntpdate

```
#!/bin/sh
#
# Datum
#

/usr/sbin/ntpdate 130.75.1.40
```

R|R|Z|N

backup

```
#!/bin/sh
#
# taeglich tar von / auf /exports/backup,
# Versionen aelter als 2 Tage loeschen.
#
umask 022

PATH=/sbin:/bin:/usr/sbin:/usr/bin
export PATH

find /exports/backup -name "*gz" -ctime +2 -exec rm {} \;
tar czf /exports/backup/home.${RANDOM}.tgz /home
tar czf /exports/backup/srv.${RANDOM}.tgz /srv
tar czf /exports/backup/${RANDOM}.tgz /boot /etc /lib /var /root /usr /bin /sbin
tar czf /exports/backup/opt.${RANDOM}.tgz /opt
```

---

logrotate

```
#!/bin/sh
#
/usr/sbin/logrotate /etc/logrotate.conf
```

R|R|Z|N

online_update

```
#!/bin/sh
#
# SuSE-online-Update security
#
online_update \
        -u ftp://ftp.rrzn.uni-hannover.de/pub/mirror/linux/suse security \
    l mail -s "`/bin/uname -n`:online_update" name@adresse
```

---

disktest

```
#!/bin/bash
#
# Nachricht Disk-Ueberpruefung
#
export PATH=/bin:/usr/bin:/sbin:/usr/sbin
#

hdparm -t /dev/hda 2>&1 >/tmp/disktest_kannweg
df 2>&1 >>/tmp/disktest_kannweg

cat /tmp/disktest_kannweg  l mail -s "`/bin/uname -n`:disktest" name@adresse
rm /tmp/disktest_kannweg
```

R|R|Z|N

rogator

```
#!/bin/bash
#
# Apache_Test auf Rechner rogator
#
export PATH=/bin:/usr/bin
#
#
cat >kannweg_egal <<EOF
# Command logfile created by Lynx 2.8.4rel.1 (17 Jul 2001)
# Arg0 = lynx
# Arg1 = -cmd_log=cmd
# Arg2 = http://rogator-serv.rrzn.uni-hannover.de
key q
key y
exit
EOF
lynx -cmd_script=kannweg_egal \
      http://rogator-serv.rrzn.uni-hannover.de \
    | grep -q TEST \
   || mail -s "rogator:httpd_laeuft_nicht" name@adresse
rm kannweg_egal
```

R|R|Z|N

scanlog

```
#!/bin/bash
#
# Nachricht, falls Rechner gescant oder Datei geaendert
#
export PATH=/bin:/usr/bin
#
grep -q scanlog /var/log/messages && \
       grep -2 scanlog /var/log/messages | strings | cut -c 1-250 \
     | mail -s "`/bin/uname -n`:scanlog" name@adresse \
   && mv /var/log/messages /var/log/messages.scan.${RANDOM} \
   && touch /var/log/messages && chmod 640 /var/log/messages

exit 0
```