# Dienstbar - aber sicher !

Internetdienste auf Linux-Servern ohne Sicherheitspannen

2. Chemnitzer Linuxtag, 11./12. 03. 2000

Alexander Schreiber
<als@thangorodrim.de>

# Was darf’s den sein ?

Welche Dienste sollen angeboten werden ?

- Oeffentliche Dienste:
  - HTTP-Server
  - FTP-Server
  - Mail-Server
  - Shell-Server
- Private Dienste:
  - Intranet HTTP-Server
  - Intranet Mail
  - Intranet Zugriff fuer Aussendienst
  - Intranet Datenbanken
  - Intranet Fileserver (Samba)

# Es funktioniert - und weiter ?

Moegliche Risiken:

- Verlust der Vertraulichkeit
- Verlust der Verfuegbarkeit
- Verlust der Korrektheit

- Speicherplattform fuer illegale Aktivitaeten
- Aenderungen an Webseiten
- Plattform fuer Angriffe auf andere Systeme
- Unauthorisierte Resourcen-Nutzung
- SPAM-Relay

# Elementare Massnahmen

Grundlagen fuer ein sicheres System:

- Stillegen ungenutzter Dienste
- Installation aktueller Software-Versionen
- genutzte Software sicher konfigurieren
- Sicherheitsmailinglisten verfolgen

# Sicherheit - Nutzbarkeit

Gratwanderung zwischen Sicherheit und Nutzbarkeit eines Systems :

- absolut sicheres System : ausgeschaltet ...
- am einfachsten : alle Dienste installieren
- Sicherheit = Aufwand (Zeit, Geld)
- aber : Kosten eines Systemeinbruchs ?

# Sicherheit braucht Planung !

Entwicklung Sicherheitsstrategie :

- Feststellung schuetzenswerter Objekte
- Ausarbeitung worst-case Szenarien
- Kostenabschaetzung worst-case

- Notwendigkeit der Sicherheit ?
- Wie sicher soll es sein ?
- Fuer Sicherheit verfuegbare Resourcen ?

# Sicherheit mit Linux

Sehr verschiedene Moeglichkeiten :

- umfangreiche Moeglichkeiten mit Bordmitteln
- gut konfiguriertes UNIX-System
- Sicherheit durch geeignete Soft/Hardware
- hohe Sicherheit bei geringen Kosten

- Loesungen von einfach bis komplex
- abhaengig von Zielen und Moeglichkeiten
- wichtig : kompetenter Admin !

# Grundsaetzliches

Standardmassnahmen fuer alle Szenarien :

- aktueller Kernel + secure-linux patch :
  - bei http://www.openwall.com
  - non-executable stack
  - restricted links in t+ dirs
  - restricted FIFO’s in t+ dirs
  - restricted /proc
  - spezielle Behandlung std(in|out|err) FD
- Systemkonfiguration :
  - Server-Software sicher konfiguriert
  - System sicher konfiguriert
  - System gehaertet (SuSE : harden_suse)
  - System physikalisch gesichert !

# Grundsaeztliches - Fortsetzung

- Volles Logging
- Logs auf sichere Ablage (Loghost)
- korrekte Systemzeit
- automatische Auswertung der Logs
- Statusmonitoring des Servers
- Anomalitaeten nachpruefen

# Beispiel : FTP-Server vor DMZ

- Massnahmen
  - Inhalte von hardware read-only medium
  - /incoming separates FS, write-only
  - sicheren ftpd nutzen
- Ergebnis
  - Inhalte nicht remote aenderbar
  - Nutzung incoming als Handelsplatz erschwert

# Beispiel : Webserver in DMZ

- Massnahmen
  - DMZ als RFC1918-Netz
  - kein direkter Zugriff auf Server
  - Firewall agiert nach aussen als Webserver
  - Port 80/443 mit Kernel-Portforwarding
  - sicher konfigurierter Apache
- Ergebis
  - auf Webserver _nur_ Apache ereichbar
  - Apache als Angriffsziel
  - auf Apache laufender Code (CGI/PHP) als Ziel
  - guenstig, relativ sicher

# Beispiel : Sicherer Webserver

- Massnahmen
  - System laeuft von hardware readonly + initrd
  - Sentinel-Host an separate Netzkarte
  - Sentinel nicht extern sichtbar
  - Sentinel checkt Inhalte, Reboot Server bei Differenz
- Ergebnis
  - Inhalte extern nicht aenderbar
  - bei Aenderung sofort zurueck auf korrekten Stand
  - Einbruch zwecklos

# Links zum Thema

- OpenWall Linux Project
  - http://www.openwall.com
- Linux IP Firewalling Chains (ipchains)
  - http://www.rustcorp.com/linux/ipchains/
- FreshMeat - Quelle Nr. 1 fuer Linuxsoftware
  - http://www.freshmeat.net