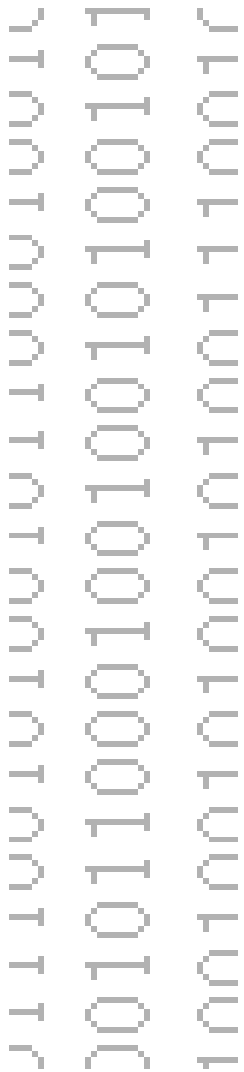
Logging, Monitoring und Auditing

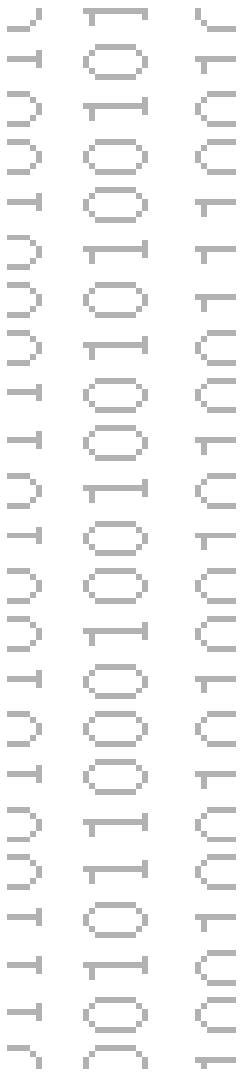
Ingo Schäfer, 29.05.2008

Ablauf des Vortrages



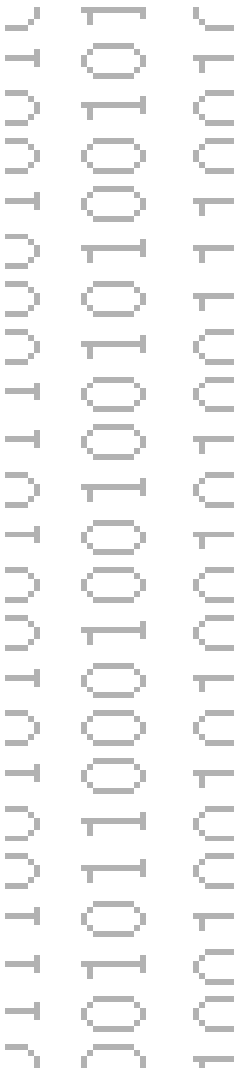
- Kernkonzepte und Begriffe
- Realisierungsmöglichkeiten
- Warum überhaupt?
- Fallbeispiele aus Literatur und Praxis

Definition Logging



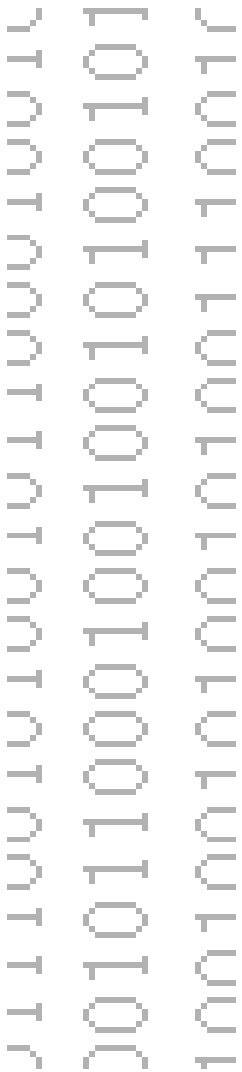
- Logging = Protokollierung
- „Logging (in any application) generally means some way to indicate the state of the system at runtime.“ (Gupta)
- Aufgabe aus der System-Administration
- Aufzeichnung von Ereignissen

Definition Auditing



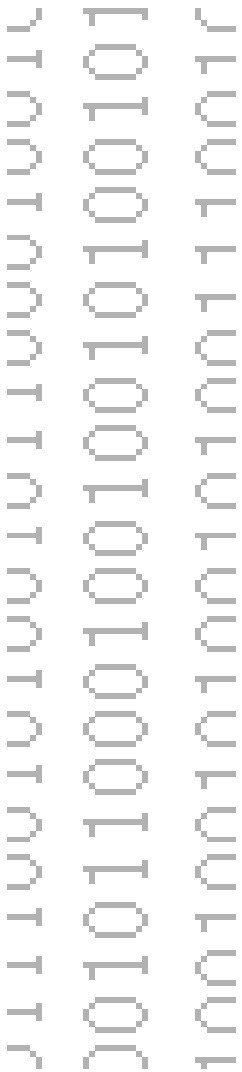
- Auditing = beweissichere Protokollierung eines Vorfalls
- Oder: Detaillierte Analyse eines Systems (z.B. auf Schwächen)
- Methodiken und Mittel sind bei beiden Zielen gleich

Definition Monitoring



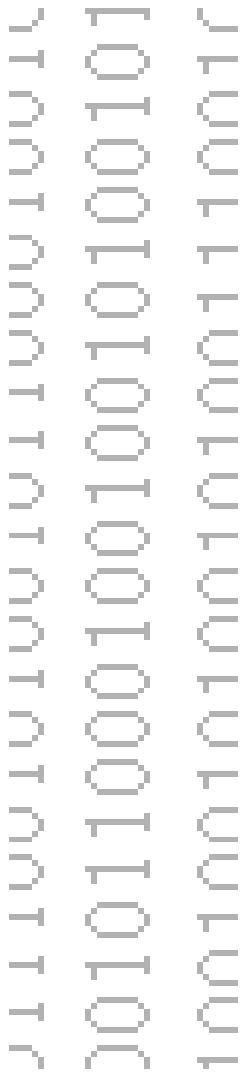
- Monitoring = Beobachtung
- Laufende Überwachung des Zustandes von Systemen und des Netzwerkes
- Um Anomalien festzustellen, muss man wissen, was „normal“ ist!
- Anomalien können ein Zeichen für Angriffe sein

Diskussion: Was ist normal?



- Fragen:
  - Sind 720 ICMP-Pakete pro Stunde vom internen Netzwerk nach „außen“ normal?
  - Ist eine kontinuierliche Datentransferrate von 500 kbit/s auf der 2 Mbit-Standleitung normal?

Logging vs. Datenschutz

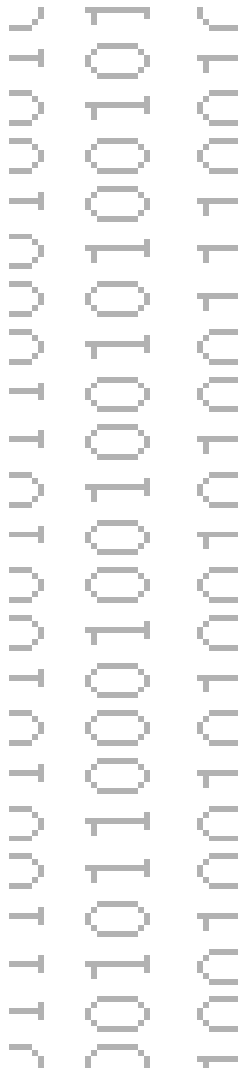


- Log-Files können personenbezogene Daten enthalten
  - Jegliche Protokollierung muss dem DSB angezeigt werden
  - Manchmal gilt daher: Weniger ist mehr
- Konfliktpotential!
  - Der Admin will möglichst alles wissen, die Nutzer möglichst viel verbergen ...
- Außerdem: Log-Files in falschen Händen können schaden

Vergleich der Verfahren

	Logging	**Monitoring**	**Auditing**
Zeitlich	Permanent	Permanent	Sporadisch
Was wird erhoben?	Ereignisse	Status	Alle relevanten Informationen
Wann angesehen?	Im Fehlerfall	Ständig	Nach Abschluss
Einrichtungsaufwand	Niedrig	Hoch	Nicht vorhanden
Durchführungsaufwand	Normal	Hoch	Sehr hoch

Logging - Realisierungsmöglichkeiten

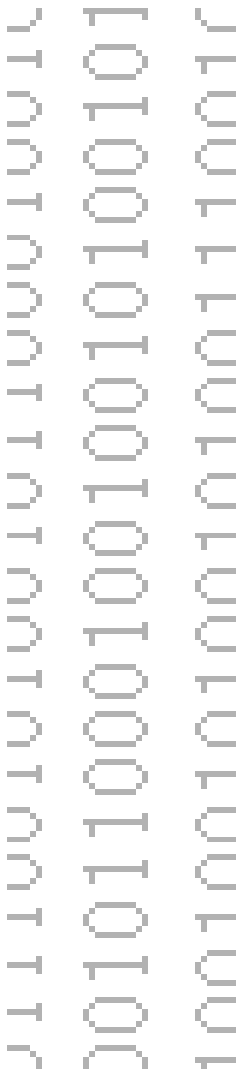


- Arten
  - Dateien
  - Datenbank-Einträge
  - Papierausdrucke
  - E-Mails und andere Nachrichten
- Klassifizierung
  - Nach Anwendung
  - Nach System
  - Global
  - Mischformen

Logging – Unix / Linux 1

- syslogd / klogd
  - Log-Dateien in `/var/log`
    und/oder in `/var/adm/log`
    und/oder ...
  - Konfiguration in `/etc/syslog.conf`
  - Zusätzlich je nach Anwendung weitere Log-Dateien üblich
  - Systemcall: `void syslog(int priority, const char *message, ...);`
  - Kommando: `logger „Nachricht“`

Logging – Unix / Linux 2



/etc/syslog.conf:

```
*.err;kern.*;auth.notice                    /dev/console

*.notice;authpriv,remoteauth,ftp,install.none; \
    kern.debug;mail.crit        /var/log/system.log

authpriv.*;remoteauth.crit    /var/log/secure.log

lpr.info                        /var/log/lpr.log
mail.*                         /var/log/mail.log
ftp.*                           /var/log/ftp.log
```

Logging – Unix / Linux 3

```
Feb 11 20:56:01 zeus sshd[12107]: [ID 702911
local6.warning] password authentication failed.
Connection from 83.218.161.25 denied.
Authentication as user root was attempted.
```

Timestamp, Hostname, Prozess [ProzessID]:

[Ereignis-ID, facility.priority] Nachrichtentext

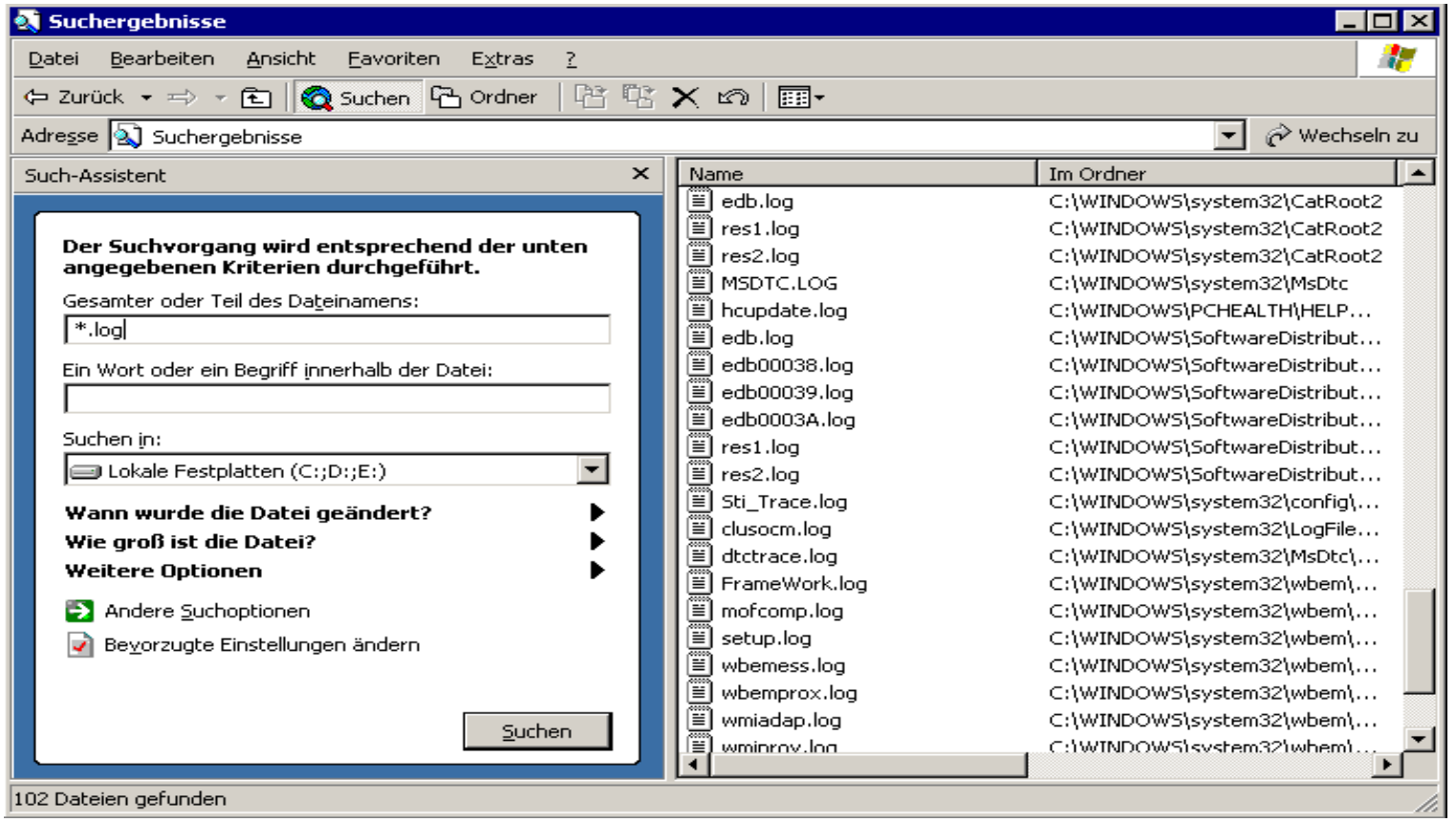
Im Beispiel: Der (erfolglose) Versuch, sich als root per ssh anzumelden.

Logging – Windows

- Ereignisprotokoll(e) / Eventlog
  - Security, System und Anwendung
  - Auf Domain-Controller zusätzlich DNS, File Replication und Directory Service
  - Liegt in binärer Form vor
- Zusätzlich noch „normale“ Log-Dateien

Logging – Windows 2

- 102 Dateien in diversen Verzeichnissen verstreut



Logging – Windows 3

- C:\Windows\Debug\cysui.log

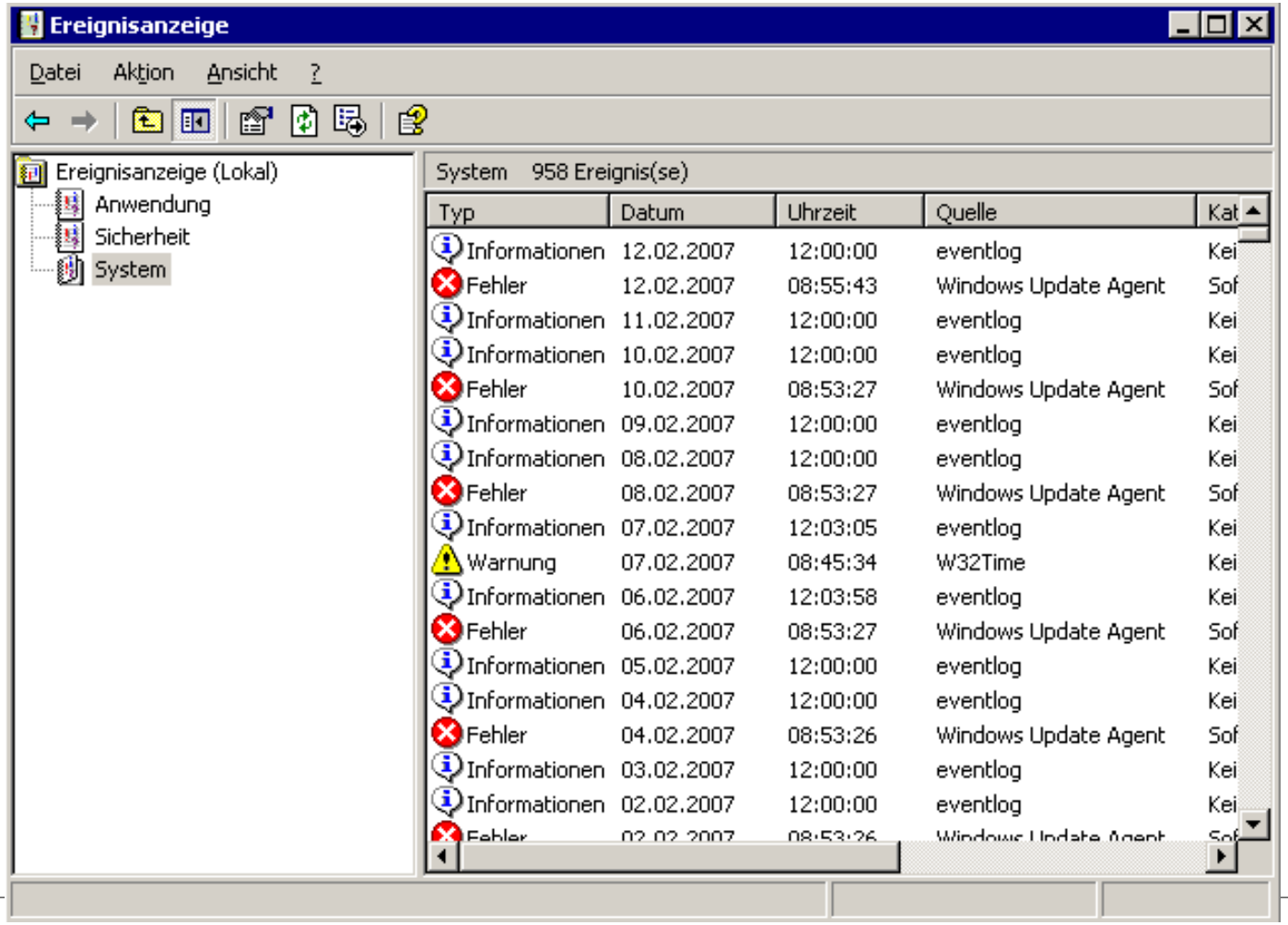
cysui.log - Editor

Datei Bearbeiten Format Ansicht ?

```
cysui 224.250 0000 00:00:01:09.0546 opening log file C:\WINDOWS\debug\cysui.log
cysui 224.250 0001 00:00:01:09.0546 C:\WINDOWS\system32\cys.exe
cysui 224.250 0002 00:00:01:09.0546 file timestamp 03/26/2003 14:00:00.000
cysui 224.250 0003 00:00:01:09.0546 local time 04/24/2006 11:10:33.937
cysui 224.250 0004 00:00:01:09.0546 running Windows NT 5.2 build 3790  (BuildLab:3790.srv03_rtm.
cysui 224.250 0005 00:00:01:09.0546 logging flags 000100BC
cysui 224.250 0006 00:00:01:09.0562 Enter Start
cysui 224.250 0007 00:00:01:09.0562   Enter IsCurrentUserAdministrator
cysui 224.250 0008 00:00:01:09.0562     Current user is an admin
cysui 224.250 0009 00:00:01:09.0562   Enter Computer::RemoveLeadingBackslashes
cysui 224.250 000A 00:00:01:09.0562   Enter Computer::Refresh
cysui 224.250 000B 00:00:01:09.0562     Enter IsLocalComputer
cysui 224.250 000C 00:00:01:09.0562     Enter RefreshLocalInformation
cysui 224.250 000D 00:00:01:09.0562     Enter GetProductTypeFromRegistry
cysui 224.250 000E 00:00:01:09.0562       Enter RegistryKey::Open System\CurrentControlSet\Contr
cysui 224.250 000F 00:00:01:09.0562       Enter RegistryKey::GetValue-String ProductType
cysui 224.250 0010 00:00:01:09.0562       ServerNT
cysui 224.250 0011 00:00:01:09.0562       prodtype : 0x3
cysui 224.250 0012 00:00:01:09.0562     Enter GetSafebootOption
cysui 224.250 0013 00:00:01:09.0562       Enter RegistryKey::Open System\CurrentControlSet\Contr
cysui 224.250 0014 00:00:01:09.0562       HRESULT = 0x80070002
cysui 224.250 0015 00:00:01:09.0562       returning : 0x0
cysui 224.250 0016 00:00:01:09.0562     Enter DetermineRoleAndMembership
cysui 224.250 0017 00:00:01:09.0562       Enter MyDsRoleGetPrimaryDomainInformation
cysui 224.250 0018 00:00:01:09.0562         Enter MyDsRoleGetPrimaryDomainInformationHelper
cysui 224.250 0019 00:00:01:09.0562           Calling DsRoleGetPrimaryDomainInformation
```

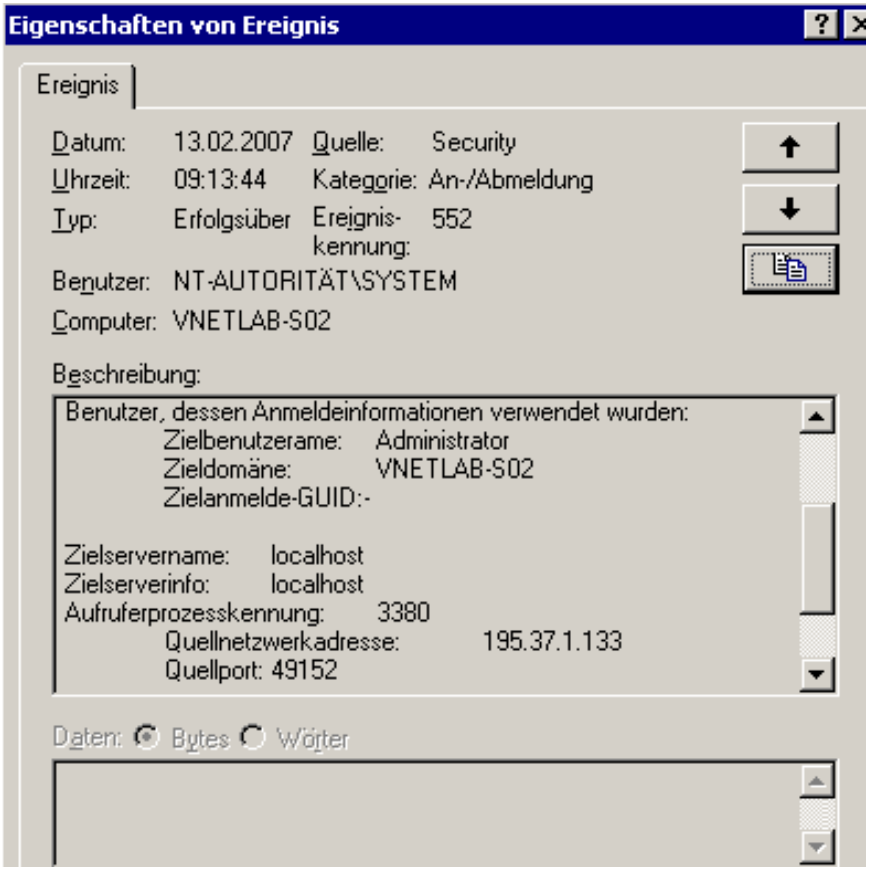
Logging – Windows 4

- Windows-Eventlog-Viewer



Logging – Windows 5

- Kategorie
- Ereigniskennung
- Quelle
- Host
- Beschreibung mit detaillierten Informationen

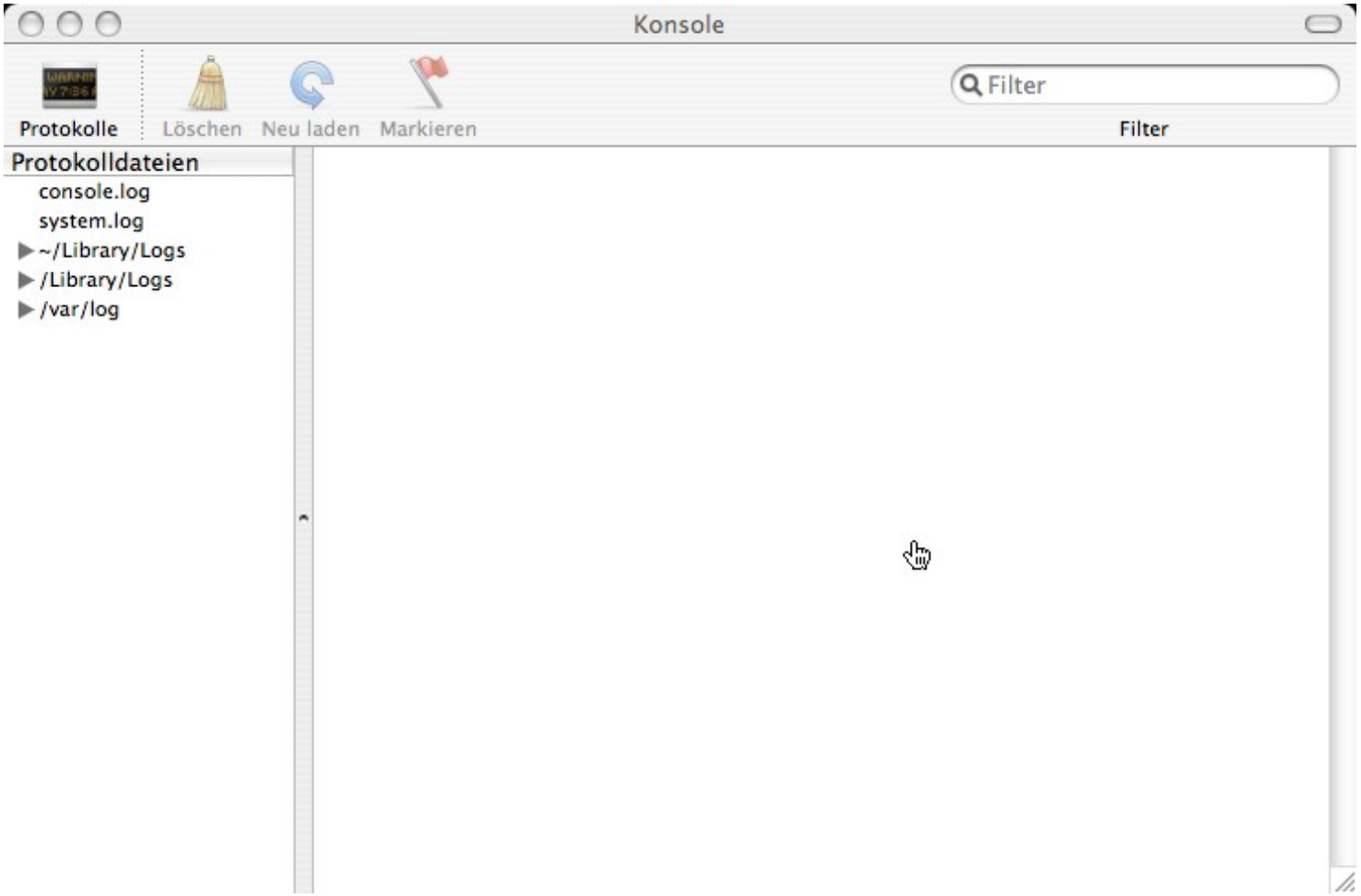


Logging – Mac OS X 1

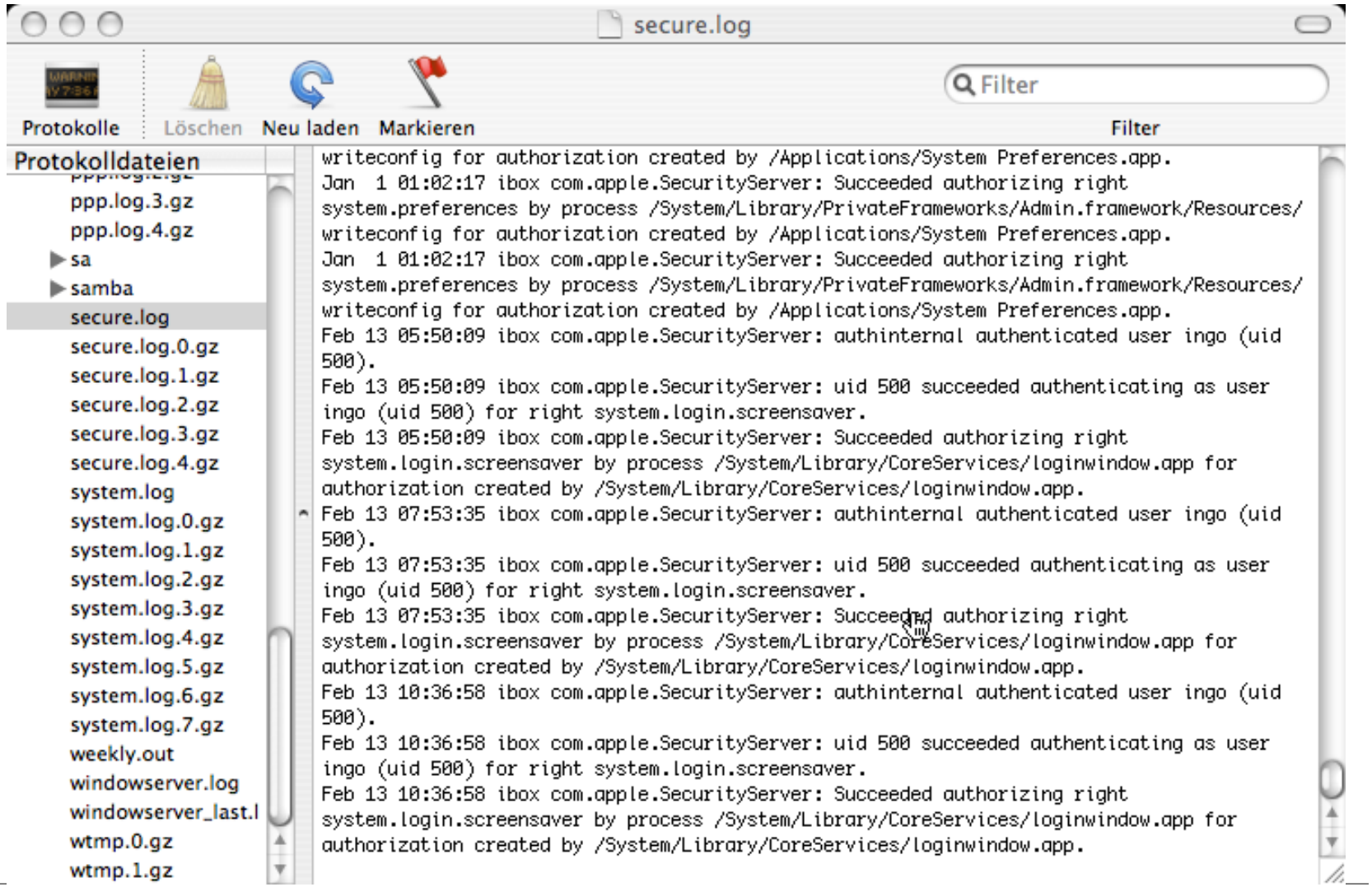
- Unix-Bestandteile protokollieren in `/var/log`
- Mac-Programme in
  - `/Library/Logs` (systemweit) bzw
  - `~/Library/Logs` (nutzerspezifisch)
- Anzeige mit „Konsole“
  - In Dienstprogramme

Konsole

Logging – Mac OS X 2



Logging – Mac OS X 3



Logging im Netzwerk

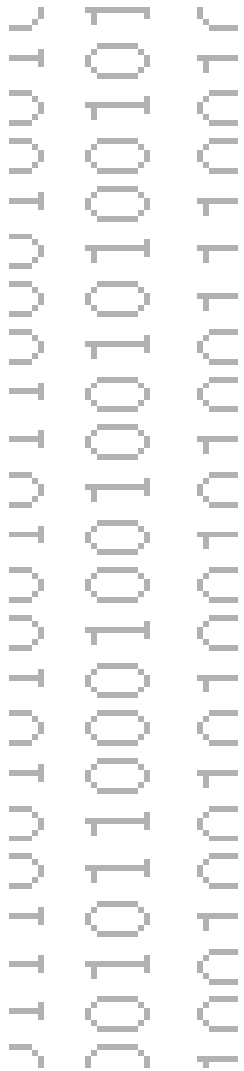
- Syslogd kann auf UDP Port 514 Meldungen entgegennehmen
- Je nach Konfiguration lokale Speicherung oder Relay
- Einige Probleme
  - Syslog-Nachrichten können verloren gehen
  - Denial of Service gegen zentralen Server macht „blind“
  - Angreifer kann eigene Log-Meldungen platzieren
  - Übertragung im Klartext
- Aber: etablierte Lösung für zentralisiertes Logging

Logging im Netzwerk – neue Ideen

- Syslog über TCP
- IPSec-Tunnel zum Log-Server
- MsysLog kann durch kryptographische Methoden nachträgliche Manipulation erkennen
- Reliable Syslog over BEEP over tcp
- Syslog-Sign

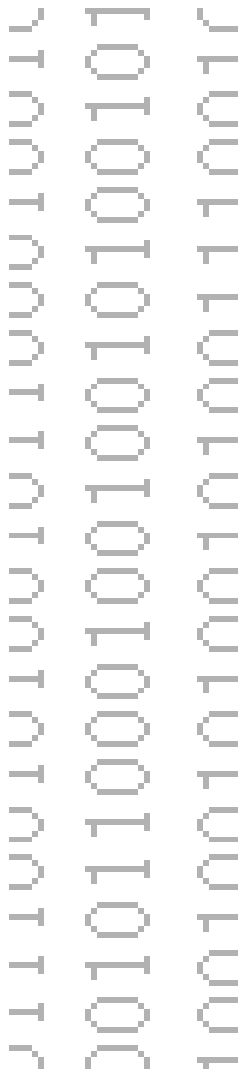
==> Verschlüsselung und Integritätssicherung können auch Netzwerklogging sicher machen

Logging - Wieviel?



- Nur das protokollieren, was man auch sehen möchte
  - Nur die Meldungen aufnehmen, mit denen man was anfangen kann
  - „Sehen Sie nur nach den Problemen, von denen Sie wissen, wie Sie diese lösen können.“
- Macht dieser Ansatz Sinn?

Log-Daten beherrschen



- Die Menge der Log-Daten ist ziemlich groß
- Protokollanalyse-Tools helfen
  - logcheck, logwatch, logsentry
  - Analysieren periodisch Log-Einträge und melden alle nicht ignorierten Einträge (z.B. per Mail)
  - Fein granulierte Filterung möglich
- Vorstufe zum Monitoring

Monitoring – Was kann man überwachen?

- Netzwerkstatus
  - Durchsatz
  - Verkehrsströme
- Host-Status
  - Auslastung
  - Speichernutzung
  - Plattenkapazität
  - Laufende Prozesse
- u.v.m.

Monitoring – Wie?

- Integrierte Tools
  - Task-Manager, top, prstat
- Protokolle wie SNMP
- Spezielle Tools
  - gkrellm(d), HP OpenView, IBM Tivoli, Mercury, Indicative Service Director, GFI LANGuard Security Event Log Monitor, Nagios u.v.m.
- Grenze zum Auditing fliessend

Monitoring – gkrellm(d)

- Open-Source-Monitoring-Tool
- Überwachung wichtiger Systemparameter
- Erweiterbar
- Client-Server-Architektur

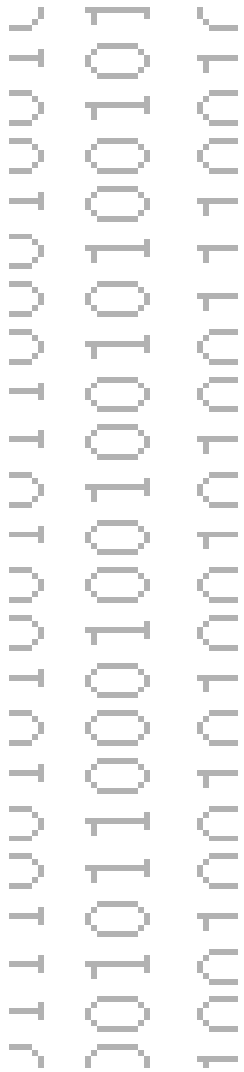
- Nur Echtzeit-Monitoring, keine Vergangenheitsdaten

- **Live-Demo**

Monitoring – gkrellm(d)

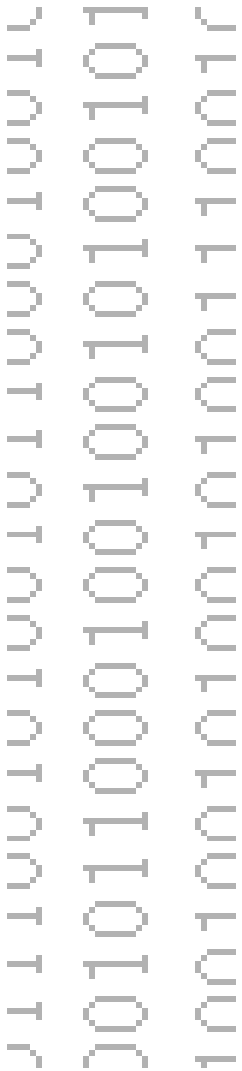
- Zwei Beispiele vom gleichen Host
- Was ist normal?
- Was ist vielleicht unnormal?
- Was ist ganz sicher unnormal?

Monitoring – SNMP 1



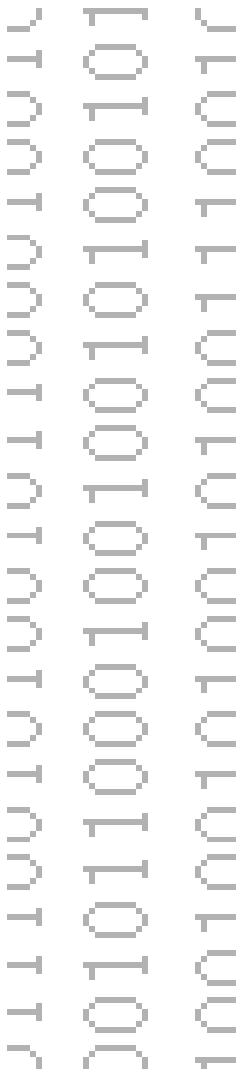
- Protokoll zum Netzwerkmanagement
- IETF-Standard RFC 1441 und folgende spezifizieren SNMPv2
- Client-Server-Protokoll
  - Manager = Software in der Management-Station
  - Agent = Software im überwachten Gerät

Monitoring – SNMP 2



- Hierarchische Informationsstruktur (MIB)
  - Object-Identifier starten mit 1.3.6.1.2.1 (mib-2)
  - Darunter dann verschiedene Untergruppen
- Viele Werte Read-Only
- Version 1 praktisch ohne Sicherheit, Version 2 besser

Monitoring – Nagios



- Freie Software zum Monitoring von Netzwerk-Diensten
- Flexibel durch Plugins
- Web-Interface, flexible Benachrichtigungen
- Jeder Wert, der digital erfasst werden kann, ist ein Messwert
  - Temperatur, Lautstärke, Neutronen
- **Live-Demo**

Auditing mit Tools

- Prozess-Accounting erleichtert nachträgliche Analyse
  - Alle laufenden Prozesse und Netzwerkverbindungen werden effizient protokolliert
  - In Linux, Solaris und BSD integriert (weiss jemand, wie das bei OSX und Windows ist)

- Aber: Ist Überwachung der Nutzer
  d.h. die Datenschutz-Problematik muss zwingend beachtet werden!

Auditing mit Tools 2

- Microsoft Baseline Security Analyzer (MBSA)
  - Analyse des Patch- und Konfigurationsstandes
- Microsoft Windows Server Update Services
  - Automatisierte Überwachung und Verwaltung der Microsoft-Updates in der gesamten Netzwerkumgebung
- Möglicherweise heissen die Teile inzwischen anders ...

Auditing mit Tools 3

- Security-Scanner wie SuperScan, nmap oder nessus
  - Port-scanning
  - Erkennen der Dienste incl. Version
  - Auswerten mit Datenbank über bekannte Schwachstellen
- Keine Aussage, ob wirklich anfällig, aber Hinweis
- Metasploit-Framework erlaubt das Ausnutzen der bekannten Sicherheitslücken

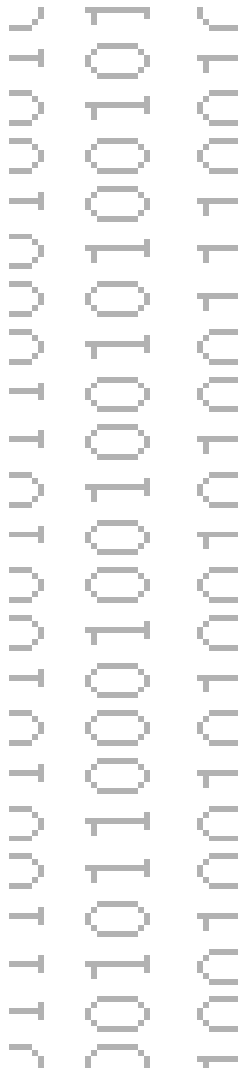
Auditing 4

- Manuelle Kontrolle der Hosts
  - Kontrolle der laufenden Prozesse
    - `ps, top, pstree, prstat`
    - Windows Task Manager
  - Kontrolle der Netzwerkverbindungen
    - `netstat, lsof`
  - Kontrolle der Einstellungen
    - Systemdienste (Startdateien etc.)
    - Einstellungen der Paketfilter

Auditing 5

- `netstat -an`
  - listet alle Netzwerkverbindungen
  - PID dazu Windows: `-o` Linux: `-p`
- `ps -aef`
  - listet alle Prozesse mit möglichst komplettem Aufruf
- `pstree`
  - listet Prozesse mit Eltern in Baumdarstellung

Auditing 6



- Integrität des Systems sicherstellen
  - `chkrootkit` oder `rkhunter` finden bekannte Root-Kits
  - `tripwire` erstellt Datenbank mit Merkmalen und Checksummen, kann diese dann mit einem laufenden System vergleichen
- saubere Datenträger verwenden

Noch Fragen, Kie^W^H^H?