



# **Workshop IT-Sicherheit**

## **10.9.2008**

### **Überwachung der Sicherheit**





# Inhalte

---

- Einführung
  - Überwachung durch Protokollierung
  - Warum Protokollierung
- Grundlagen
  - Unix / Linux
  - Windows
  - Cisco
- Umsetzung im Unternehmen
- Fazit



# Überwachung durch Protokollierung

---

Protokollierung

=

Aufzeichnung von stattgefundenen Ereignissen

Überwachung

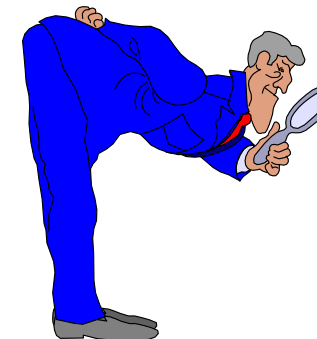
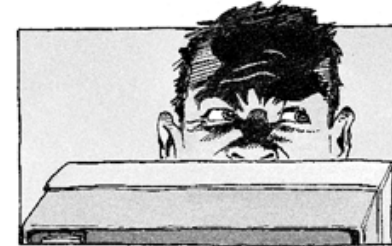
=

Regelmäßige Auswertung der Aufzeichnungen



# Warum Protokollierung

- Frühzeitige Entdeckung von sicherheitsrelevanten Vorfällen
  - komprimierte Auswertungen ausgewählter Ereignisse sinnvoll
  
- Untersuchung erfolgter Vorfälle
  - umfangreiche Protokolldaten sinnvoll
  - Korrelation unterschiedlicher Quellen





# **Grundlagen**

## **Unix / Linux**

## **Windows**

## **Cisco**



# Grundgedanken

- Zentrale Sammlung der Protokolldaten auf einem „Protokoll-Server“
- Verwendung des Syslogs-Standards als gemeinsames Format
  - entstanden aus dem UNIX-Umfeld
  - nutzt UDP / IP Protokoll
  - Aufbau der Syslog-Nachricht

<b>Feld</b>	<b>Inhalt</b>
Time stamp	z.B. 2007-06-20 13:54:05
Severity	0 Emergency / 1 Alert / 2 Critical / 3 Error / 4 Warning / 5 Notice / 6 Informational / 7 Debug
Facility	0 – 23, z.B. 0 kernel messages / 1 user-level messages / 2 mail system / local 0 – local 7
Sender	IP-Adresse oder DNS-Name
Text	Beschreibung des Ereignisses

Priority



## Bsp. LINUX-Einstellungen

- Ausgewählte Facilities: z.B. Auth, Authpriv zur Überwachung von Logins
  - Wird direkt als Facility in der Syslog-Message eingetragen
- Logging Einstellungen werden in der Datei /etc/syslog.conf vorgenommen
  - `auth,authpriv.*` `@<Adresse Log-Server>`



# Windows - Ereignisse

**Ereignisanzeige**

Datei Aktion Ansicht ?

Ereignisanzeige (Lokal)

- Anwendung
- Sicherheit
- System
- Verzeichnisdienst
- DNS-Server
- Dateireplikationsdienst

Name	Typ	Beschreibung	Größe
Anwendung	Prot...	Anwendungsfehlereinträge	192,0 KB
Sicherheit	Prot...	Sicherheitsüberwachungseinträge	64,0 MB
System	Prot...	Systemfehlereinträge	1,0 MB
Verzeichnisdienst	Prot...	Benutzerdef. Protokollfehlereinträge	192,0 KB
DNS-Server	Prot...	Benutzerdef. Protokollfehlereinträge	64,0 KB
Dateireplikationsdienst	Prot...	Benutzerdef. Protokollfehlereinträge	

**Ereignisanzeige**

System 6.816 Ereignis(se)

Typ	Datum	Uhrzeit	Quelle	Kategorie	Ereignis	Ber...
Info	13.08.2008	19:09:55	Print	Keine	42	SY...
Info	13.08.2008	19:09:45	Print	Keine	9	SY...
Info	13.08.2008	19:09:44	Print	Keine	9	SY...
Info	13.08.2008	19:09:44	Print	Keine	9	SY...
Info	13.08.2008	19:09:39	Print	Keine	9	SY...
Info	13.08.2008	19:09:39	Print	Keine	2	SY...
Info	13.08.2008	19:09:38	Print	Keine	9	SY...
Info	13.08.2008	12:06:03	Service Control Manager	Keine	7036	Nic...
Info	13.08.2008	12:03:03	Service Control Manager	Keine	7036	Nic...

**Eigenschaften von Ereignis**

Ereignis

Datum: 13.08.2008 Quelle: Service Control Manager

Uhrzeit: 12:06:03 Kategorie: Keine

Typ: Information Ereignis-kennung: 7036

Benutzer: Nicht zutreffend

Computer: T0501-SERV

Beschreibung:

Dienst "Microsoft Software Shadow Copy Provider" befindet sich jetzt im Status "Beendet".

Weitere Informationen über die Hilfe- und Supportdienste erhalten Sie unter <http://go.microsoft.com/fwlink/events.asp>.

Daten:  Bytes  Wörter

OK Abbrechen Übernehmen



# Windows Ereignis - Beispiel

Ereignistyp:	Success Audit
Ereignisquelle:	Security
Ereigniskategorie:	An-/Abmeldung
Ereigniskennung:	551
Datum / Zeit:	Mon Jun 11 14:34:24 2007
Benutzer:	mustermann
Computer:	TESTRECHNER
Beschreibung:	Benutzerinitiierte Abmeldung: Benutzername: mustermann Domäne: MUSTERFIRMA Anmeldekennung: (0x0,0x33a20ae) 2

- Umwandlung in Syslog nur mit spezieller SW
  - sehr lange Windows-Ereignistexte werden durch das Syslog-Protokoll abgeschnitten (z.B. 642: sicherheitsrelevante Änderung eines Benutzerkonto )



# Bsp. Win-Überwachungseinstellungen Sicherheit

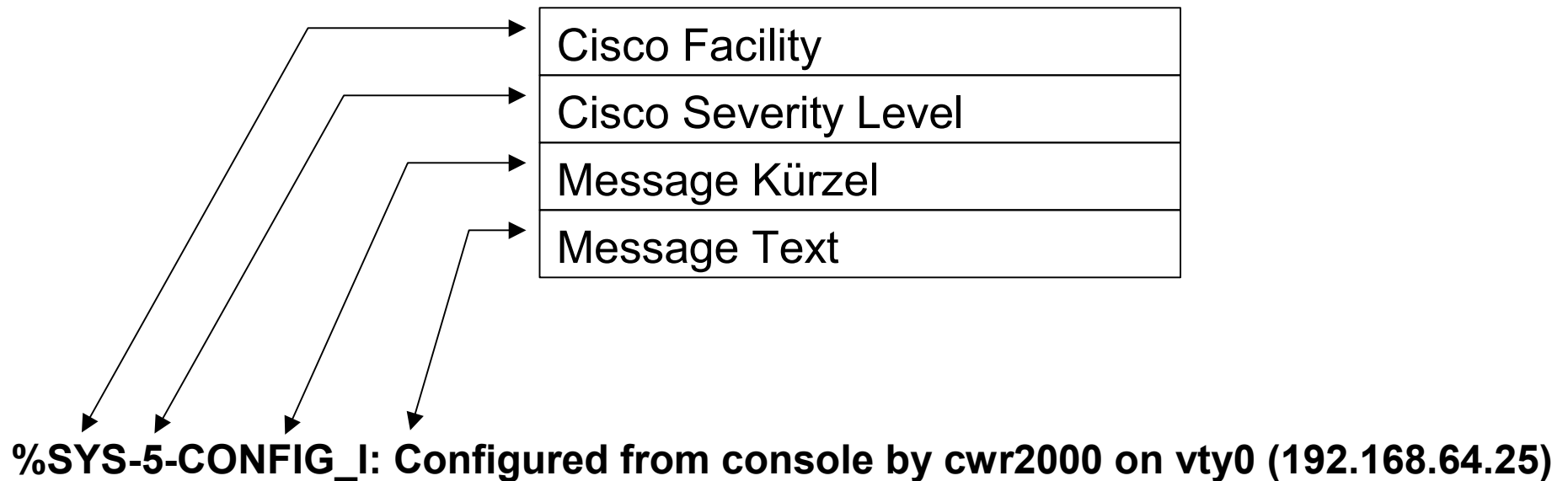
- Verwendung der Sicherheits-Ereignisüberwachung von Windows
- Konfiguration über Richtlinien-Verwaltung

<b>GrpID</b>	<b>Ereignisgruppe</b>	<b>Erfolg</b>	<b>Fehler</b>
AmE	Anmeldeereignisse überwachen (lokal)	Ja	Ja
AmV	Anmeldeversuche überwachen (NW)	-	Ja
ADZ	AD-Zugriff überwachen	-	-
Kto	Kontenverwaltung überwachen	Ja	-
Obj	Objektzugriffsversuche überwachen	-	-
Rtl	Richtlinienänderung überwachen	Ja	-
RtV	Rechteverwendung überwachen	-	-
Prz	Prozessverfolgung überwachen	-	-
Sys	Systemereignisse überwachen	Ja	-



# Cisco Message

- Cisco Message Format
- mehr als 300 Facilities können geloggt werden
- kann als Syslog verschickt werden, Daten werden in der Syslog-Nachricht als Textfeld angezeigt





# Cisco IOS-Konfiguration – Router (IOS)

logging on	schaltet das logging ein
logging <aaa.bbb.ccc.ddd>	IP Adresse des Syslog-Servers
logging facility <xyz>	Zuordnung der Syslog-Facility xyz
logging rate limit all <nn>	Max. <i>nn</i> Nachrichten / sec
service timestamps log datetime [msec] [localtime] [year]	Format des Zeitstempels
logging source interface <i>interface</i>	alle messages werden mit der IP-Adresse von <i>interface</i> gesendet (loopback0)
logging trap <n >	loggt nur Events mit Severity-Level <= <i>n</i>
login on-failure log	generiert Logging-Nachrichten bei fehlerhafter Anmeldung (ab IOS 12.3T)
login on-success log	generiert Logging-Nachrichten bei erfolgreicher Anmeldung (ab IOS 12.3T)



# Cisco Severity Levels

<b>Cisco Severity Level Name</b>	<b>Cisco Severity Level Nr.</b>	<b>Beschreibung</b>	<b>Syslog Definition</b>
emergencies	0	System unbrauchbar	LOG_EMERG
alerts	1	Sofortige Maßnahme notwendig	LOG_ALERT
critical	2	Kritischer Zustand	LOG_CRIT
errors	3	Fehler-Zustand	LOG_ERR
warnings	4	Warnung	LOG_WARNING
notifications	5	Sigifikanter Normalzustand	LOG_NOTICE
informational	6	Nur zur Information	LOG_INFO
debugging	7	Debugging-Nachricht	LOG_DEBUG



# Bsp. ausgewählte Cisco Facilities

<b>Code</b>	<b>Facility</b>
SYS	Operating system
SEC_LOGIN	Cisco IOS Login Enhancements (ab IOS 12.3T)



# Umsetzung

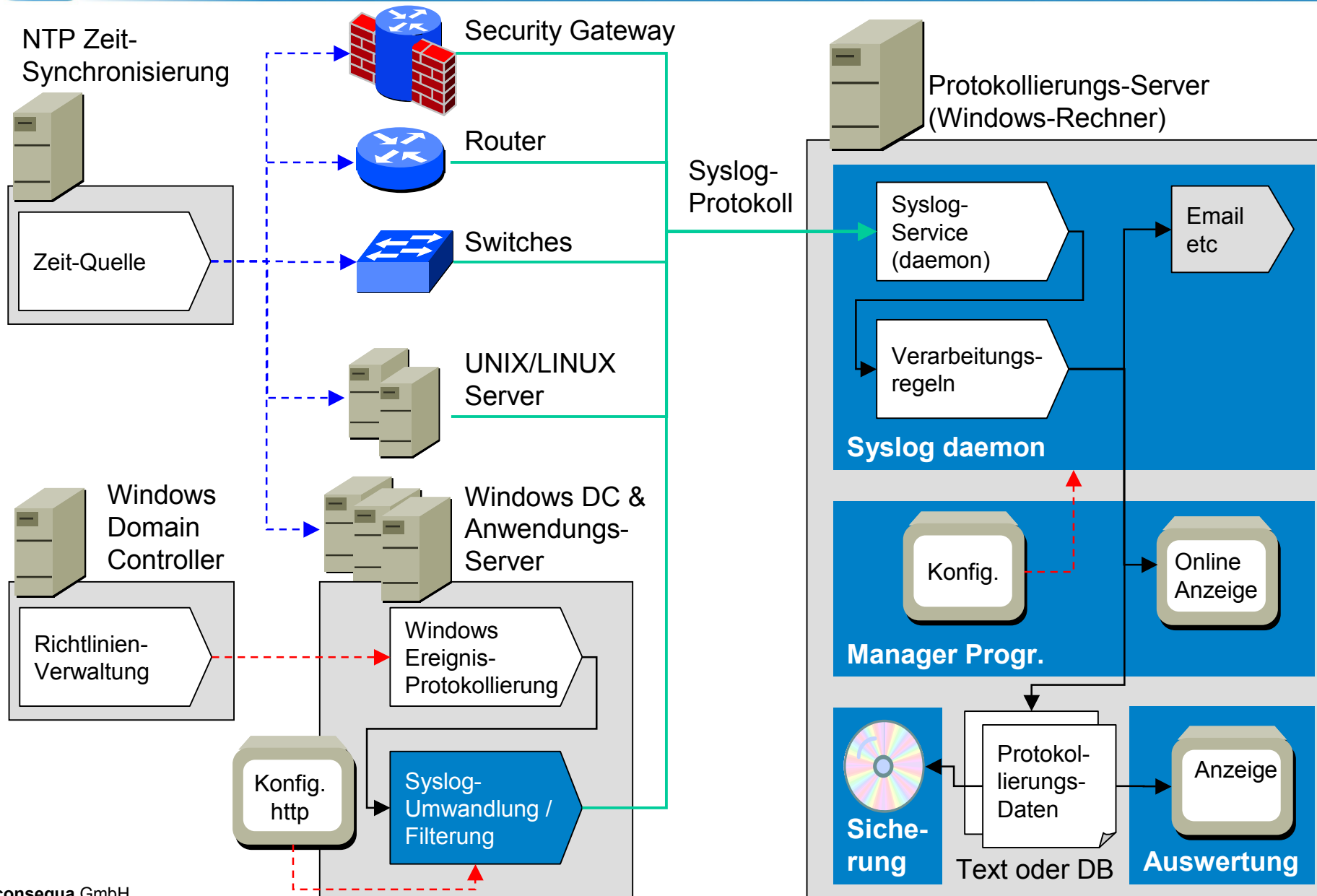


# Protokollierungskonzept

- Überwachte Systeme und Anwendungen
- Überwachte Ereignisse, z.B.
  - An- und Abmeldung (Erfolg und Fehler)
  - Systemverwaltungsaktivitäten
  - HW- / SW-Fehler
  - Zugriff auf sensible Daten
  - Verletzung von Filterregeln
- Speicherung der Protokolle
  - Manipulationssicherheit
  - Rückverfolgbarkeit
  - Gesetzliche Anforderungen (Archivierung)
- Auswertung der Protokolle
- Datenschutz-Aspekte
- Technisches Konzept
  - Protokolle
  - Werkzeuge / Systeme
  - Zeitliche Synchronisation
- Change Management



# Beispiel technisches Konzept





# Fazit



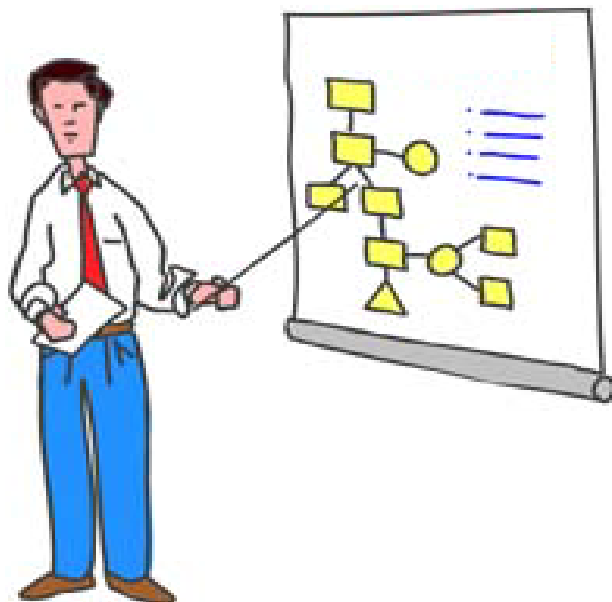
# Fazit

---

- Protokollierung ist sinnvoll
- zum Nachvollziehen von Sicherheitsvorfällen sind umfangreiche Protokollierungsdaten sinnvoll – aber Datenlawine vermeiden
- Logdaten zeitlich synchronisieren und zentral sammeln
- zur frühzeitigen Entdeckung von Sicherheitsvorfällen, komprimierte Auswertungen erstellen
- klein anfangen, Erfahrung sammeln und ausbauen
- danach strategisch vorgehen, Konzept erstellen
- auch mit geringen Mitteln lässt sich eine Menge erreichen



# Vielen Dank für Ihre Aufmerksamkeit!



Dipl.-Ing.

**Stefan Gunzelmann**

Geschäftsführer

consequa GmbH  
Süderstraße 73  
20097 Hamburg  
[www.consequa.de](http://www.consequa.de)

Tel.: 040 / 78 89 70 63  
Fax: 040 / 78 89 70 66

[stefan.gunzelmann@consequa.de](mailto:stefan.gunzelmann@consequa.de)