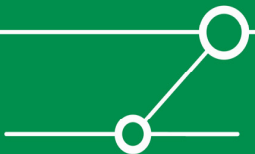


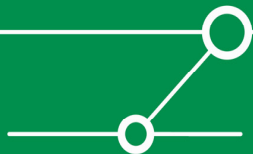
# **Voice over IP**

## **Erfahrungsbericht über Implementierung einer Open Source VoIP Telefonanlage**

**Frank Dölitzscher**



- Gegründet Sommer 2001 durch Enno Rey
- Netzwerk-Dienstleister mit Sicherheits-Fokus
- Aktuell 11 Mitarbeiter
- Schwerpunkte: Security Management, Audit/Revision, Security Research, Penetrations-Tests
- Kunden: Industrie, Banken, Behörden, Provider, Mittelständler

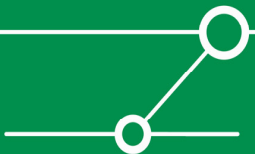


# Vorstellung Frank Dölitzscher



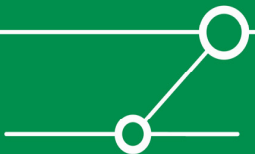
- Studium Computer Networking an der Fachhochschule Furtwangen
- Abschluss Dipl. Inform. FH August 2005
- IT-Security Trainer und Consultant bei ERNW
  
- Erfahrung im Bereich VoIP
  - VoIP Projekt im Rechenpool der Hochschule mit H.323
  - Diplomarbeit 03/2005 – 08/2005:

*„Planung und Realisierung einer Voice over IP Telefonanlage mit neusten Technologien in einem bestehenden IP Netzwerk“*



# Agenda

1. Ziel des Vortrages
2. Ausgangssituation
3. Auswahl Open Source VoIP Anlagen
4. Asterisk
5. Endgeräte
6. Zielsituation & umgesetzte Verbesserungen
7. VoIP-Security
8. Ausblick
9. Zusammenfassung

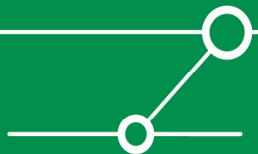


# Ziel des Vortrags



- Erfahrungen einer Umstellung weitergeben
- Probleme aufzeigen, die vorher nicht so offensichtlich sind
- Eine Ratschlag geben, für wen sich eine Umstellung auf VoIP lohnen kann

Der Fokus liegt auf der Open Source Software Asterisk, Probleme und Vorkehrungen gelten jedoch auch für andere Anlagen

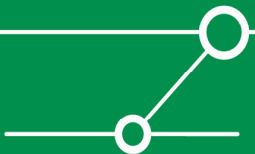
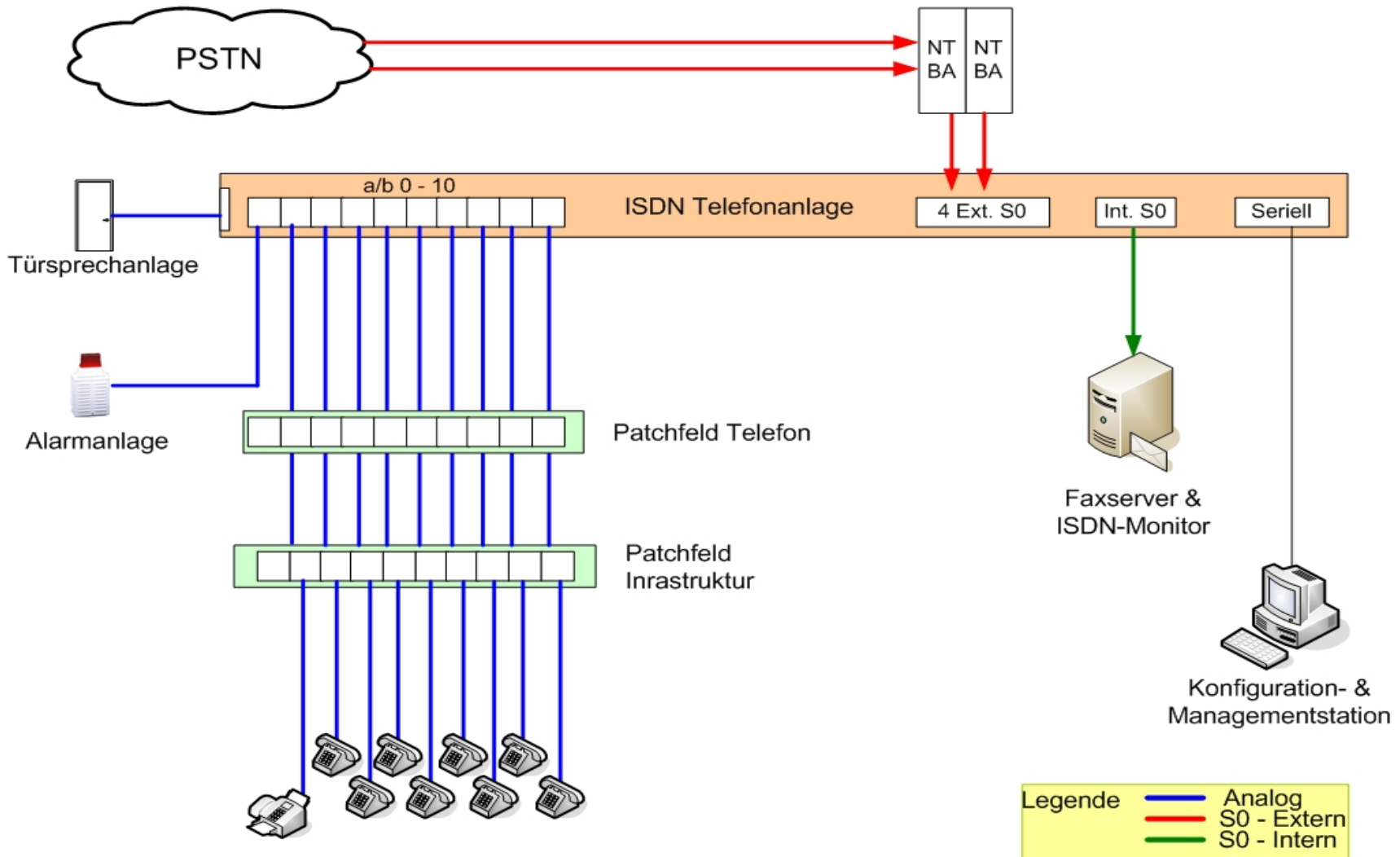


# Ausgangssituation

- IT-Serviceunternehmen
- Bestehende TK-Infrastruktur:
  - 1 ISDN Anlage
  - 1 Anlagenanschluss mit 2 NTBAs = 4 B-Kanäle
  - 10 Analoge Endgeräte (Telefone, Papierfax, Alarmanlage)
  - 1 Türfreisprechmodul
  - 1 interner S0 Bus für:
    - Faxserver
    - Anrufbeantworter (vbox-Paket)
    - ISDN-Monitorsoftware



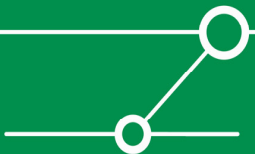
# Typische Anlagenstruktur



# Anforderungen VoIP-Anlage

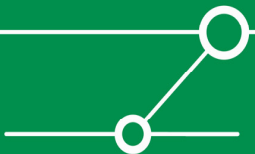


- Basis Funktionen bleiben erhalten
  - Alle vorhandenen Features einer ISDN-Anlage
  - Durchwahlen, Zentrale, Makeln, Weiterleiten ohne / mit Nachfrage, CLIP
  - S0-Bus für Faxserver & ISDN Monitor
  
- Erweiterungen / Komfortfunktionen
  - Integrierter Anrufbeantworter
  - Webinterface
  - Auswertungen
  - Kostenlose Telefonie zu Home Office



# Auswahl VoIP-Anlagen

- Kommerzielle Produkte:
    - Swyx
    - Alcatel
    - Siemens
- } Anschaffungskosten,  
Closed Source
- Freie Produkte / Open Source:
    - Bayonne
    - SIP Express Router (SER)
    - Asterisk



- **Bayonne**

IVR-Plattform um Telefonanlagenfunktionen erweitert

Minimaldokumentation vorhanden

Unterstützt als VoIP Protokoll nur H.323

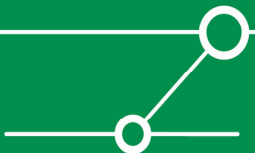
- **SIP Express Router (SER)**

Entwickelt von iptel (Arbeitsgruppe des Fraunhofer Institut)

Einfache Installation, einfache Konfiguration

Gute Dokumentation

Beschränkt auf SIP Protokoll



# Open Source VoIP-Anlagen (Fortsetz.)

- **Asterisk**

Entwickelt von Marc Spencer, Digium Inc.

VoIP Protokolle SIP, IAX(2), Skinny, H.323

Konventionelle Systeme (ISDN) leicht integrierbar

Sehr gute Dokumentation

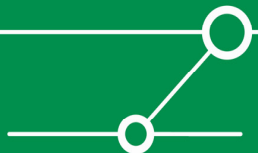
Große, aktive Entwicklergemeinde

Frei konfigurierbarer Wählplan, auch uhrzeitabhängig

Integriertes Voicemailsysteem

Datenbankanbindung an MySQL und ODBC

Verwendbar von SoHo bis Callcenter



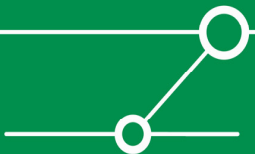
- **Hardphones**

- Analog – IP Wandler (ATA für SIP / IAX)
- SIP / IAX Telefone



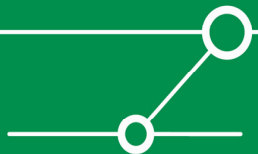
- **Softphones**

- Firefly
- X-Lite



# Umsetzung mit Asterisk

- Anbindung PSTN mit 4-Port ISDN Karte
- PBX Funktionen vollständig erhalten
- Anbindung des Faxservers und ISDN-Monitors
- Voicemailsysteem mit individuellen Voicemailboxen
- Webinterface:
  - Telefonsteuerung
  - Anruf aus Browser aufbauen
  - Anruflisten mit 1-Klick Call Funktion
- Anbindung Home Office mittels VPN



# Umsetzung mit Asterisk (Fortsetz.)

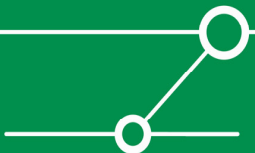
## Anrufliste im Webinterface für Admin Benutzer

Bitte wählen Sie einen Tag und eine Durchwahl aus:

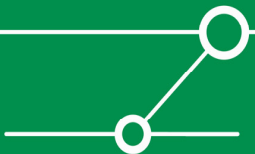
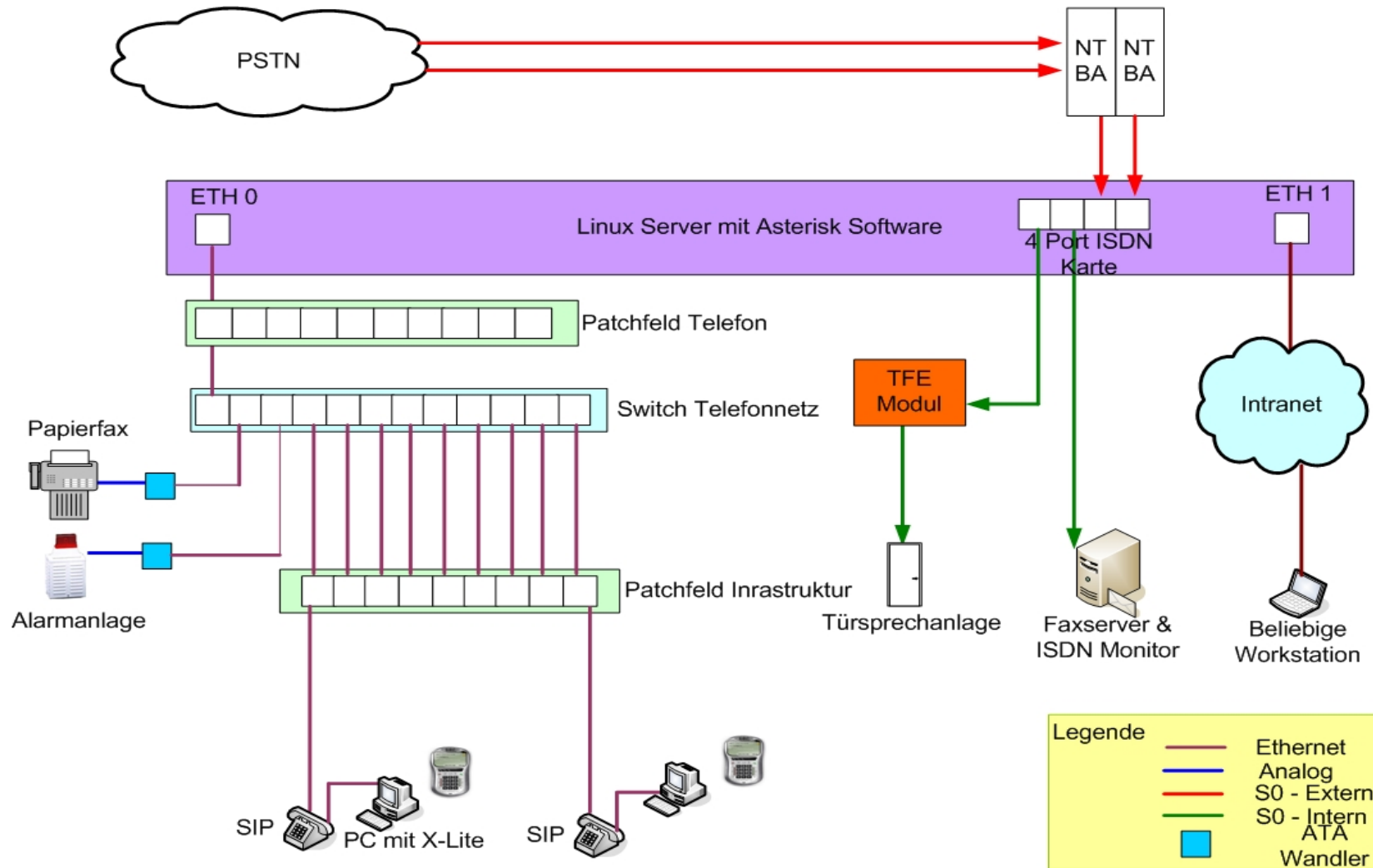
Durchwahl:  Tag:  Monat:  Jahr:

Abfrage starten

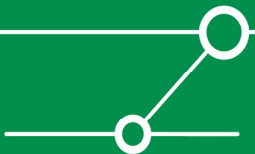
Datum	Anrufer	Ziel	Caller ID	Anrufdauer gesamt in Sekunden	Telefon Klingelzeit in Sekunden	Ergebnis
2005-08-18 17:49:51	<u>44</u>	77	44	24	21	ANSWERED
2005-08-18 17:47:59	<u>66</u>	77	66	22	14	ANSWERED
2005-08-18 17:46:57	<u>66</u>	77	66	30	30	NO ANSWER
2005-08-18 16:29:21	77	<u>66</u>	"77" <77>	1	1	NO ANSWER
2005-08-18 16:20:13		77	Test1	0	0	ANSWERED
2005-08-18 16:19:56	77	<u>66</u>	"77" <77>	1	1	NO ANSWER
2005-08-18 16:11:01	77	77	"77" <77>	2	2	NO ANSWER
2005-08-18 16:03:14	77	<u>66</u>	"77" <77>	3	3	NO ANSWER



# Struktur der Anlage mit VoIP



- **Zieldefinition**
  - Was will ich überhaupt?
  - Was brauche ich?
- **Historisch gewachsene TK-Konfiguration**
  - Verwaiste Durchwahlen
  - Veraltete Gruppen
  - Undurchsichtigkeit des Wählplans
- **Analyse der bestehenden Infrastruktur**
  - Erfassung aller Geräte
  - Erfassung aller Funktionen



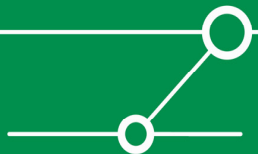
# Probleme (Fortsetz.)

- **Hard facts**

- Datenblätter vs. Kundenwerbung
- Unvollständige Implementierung von Funktionen
- Qualitätspotentiale

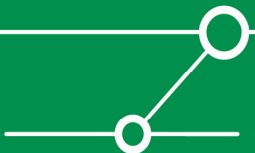
- **Soft facts**

- Design
- Sprachqualität
- Bedienung
- Umgewöhnung



- **Allgemeine Probleme von VoIP**

- VoIP benötigt eine hochverfügbare Basis
- Bandbreiten müssen vorhanden sein
- VoIP ist nicht abhörsicher
- Notruf
  - Nur lokal realisierbar
  - Aussenmitarbeiter nicht ortbar
  - Rufnummern der Einsatzleitzentralen sind nicht öffentlich
  - Bsp. VoIP-Provider sipgate



## Angriffsmethoden

- **Sniffing**

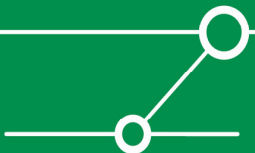
RTP ist unverschlüsselt, tcpdump + vomit bilden hier eine mächtige Waffe

- **Denial-of-Service**

möglich gegen Protokolle (meist SIP), Komponenten oder Endgeräte

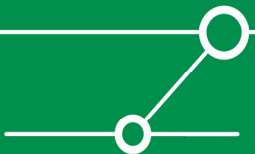
- **Angriffe gegen Management**

möglich durch fehlende Sicherheitsfeatures oder schlechte default-Konfiguration der Endgeräte => Erinnerung an die Anfänge der WLAN Access Points



## Gegenmassnahmen

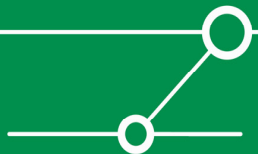
- **Segmentierung**
  - Trennung des Daten- & VoIP-Verkehrs
  - Einsatz intelligenter Firewalls, die VoIP Protokolle kennen
  
- **Verschlüsselung**
  - SRTP ist inzwischen produktionsreif
  - Externe Anbindung durch IPSec VPNs
  
- **Authentifizierung**
  - Endgeräte anhand MAC-Adresse oder Zertifikat authentifizieren



# Für wen lohnt sich der Umstieg ?

- ✓ Bevorstehende Ablösung einer bestehenden Anlage
- ✓ Verschlinkung der Infrastruktur
- ✓ Expansion
- ✓ Unternehmen mit flexibler Arbeitsplatzgestaltung
- ✓ Unternehmen, die Telefonkomfort verbessern wollen
- ✓ Parallelbetrieb zur Know-How Gewinnung

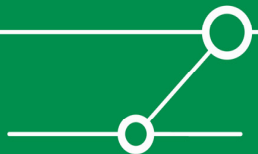
➤ ***sanfte Migration***



# Zukünftige Entwicklungen



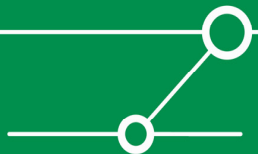
- Notrufproblematik
- Sicherheit des Sprachverkehrs
- ENUM
- SPIT = Spam over Internet Telephony
  
- Im privaten Bereich:
  - Trennung des Internetzugangs vom Telefonanschluss



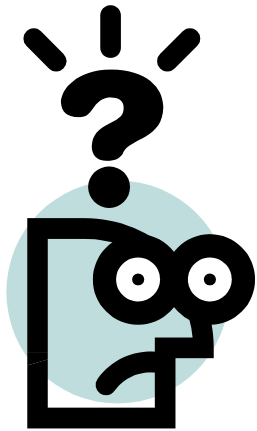
# Zusammenfassung



- VoIP ist bereit zum produktiven Einsatz
- Deutliche Komfortverbesserungen bei Telefonie
- Eine Umstellung lohnt sich bereits heute
- Gute Vorbereitung und klare Anforderungsliste erleichtern die Implementation
- Expertensupport u.U. empfehlenswert
- Sanfte Migration als Alternative zum „harten“ Umschalten verringert Risiken und senkt Hemmschwelle



**Vielen Dank für Ihre Aufmerksamkeit**



Fragen?

... und Antworten

