Voice over IT

Führt Konvergenz einer Technologie zu Divergenz beim Risiko?

Worum es geht – der Überblick

- Informations-Telefonie (IT)
- Integration in “Infrakultur”
- Sicherheit und Risiken
- Anleitungen für Skeptiker
- Strategien zur Schadensbegrenzung

Begriff *Sicherheit*

- Begriff *Sicherheit* umfaßt bis Ende des Vortrags die
  - Integrität der Verbindungs-/Gesprächsdaten
  - Vertraulichkeit der Verbindungs-/Gesprächsdaten
  - Identität der Gesprächsteilnehmer
  - Verfügbarkeit der Infrastruktur

Bedrohungsszenarien

Geschäftsmodell für Startups

a)Gründe Firma als VoIP Dienstleister

b)“Networking” mit anderen VoIP Firmen

c)“Modifizieren” von Geräten in deren Netzwerk

d)Dirigieren aller Anrufe über fremde Netze

e)Rechnungen für Dienste stellen, die andere bezahlen

“It's so easy a caveman can do it.”
-- Robert Moore, Techniker, verhaftet

Geschäftsmodell für Provider

- Telecom Italia
  “Prosecutors say the spy ring taped the phone conversations of politicians, industrialists and even footballers.” -- BBC Artikel (21.9.2006)
- Nutzen vorhandener Technik
  “According to Telecom Italia's own investigation, their procedure and machines used for the legal wiretaps had a number of flaws and it was technically possible to spy on the telephone conversations, without leaving any trace.” -- EDRi-Gram #4.15

Geschäftsmodell für Unbekannte

- Ericsson entdeckt am 4. März 2005 trojanische Pferde im Lawful Interception Subsystem von Vodafon Greece.
- Kostas Tsalikidis, Leiter Network Design bei Vodafon Greece, erhängt sich am 9. März 2005
- Vodafon deaktiviert Subsystem und löscht versehentlich alle Logs und Spuren.
- Software im Subsystem hörte Telefonate von über 100 Regierungsmitgliedern ab.
- Täter sind unbekannt.
- Quelle: The Athens Affair (IEEE Spectrum, Juli 2007)

Schlußfolgerungen aus Beispielen

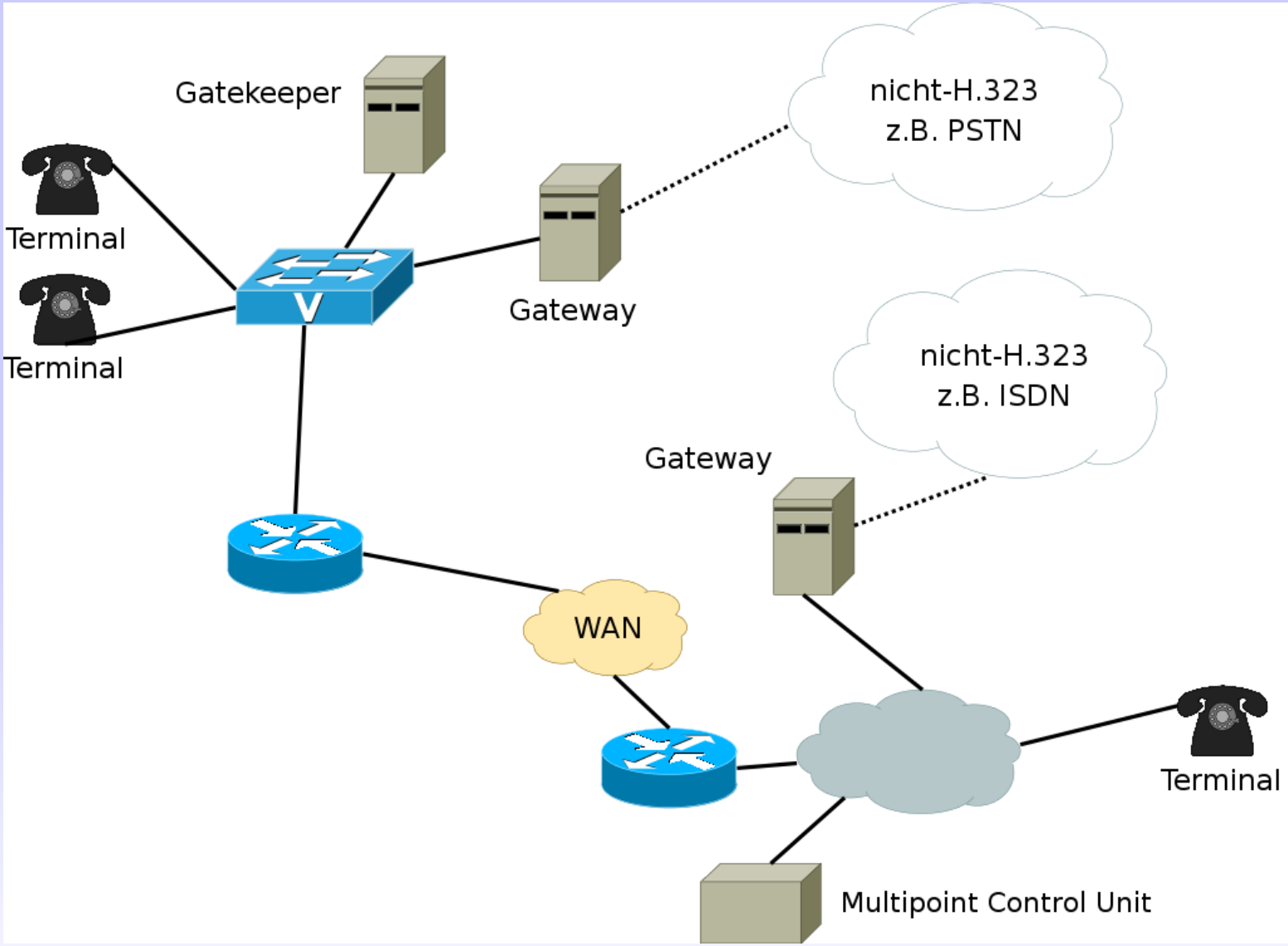
Sicherheit und analoge Telefonie

- Endgeräte besitzen (kaum) Schutzmechanismen
- Telefonanlagen ebenso
- Zugang zu PSTN und Mobilnetzen beschränkt
  - “Geringe” Zahl von Providern
  - Authentisierung beschränkt auf Anschluß
  - GSM benutzt Smart Cards

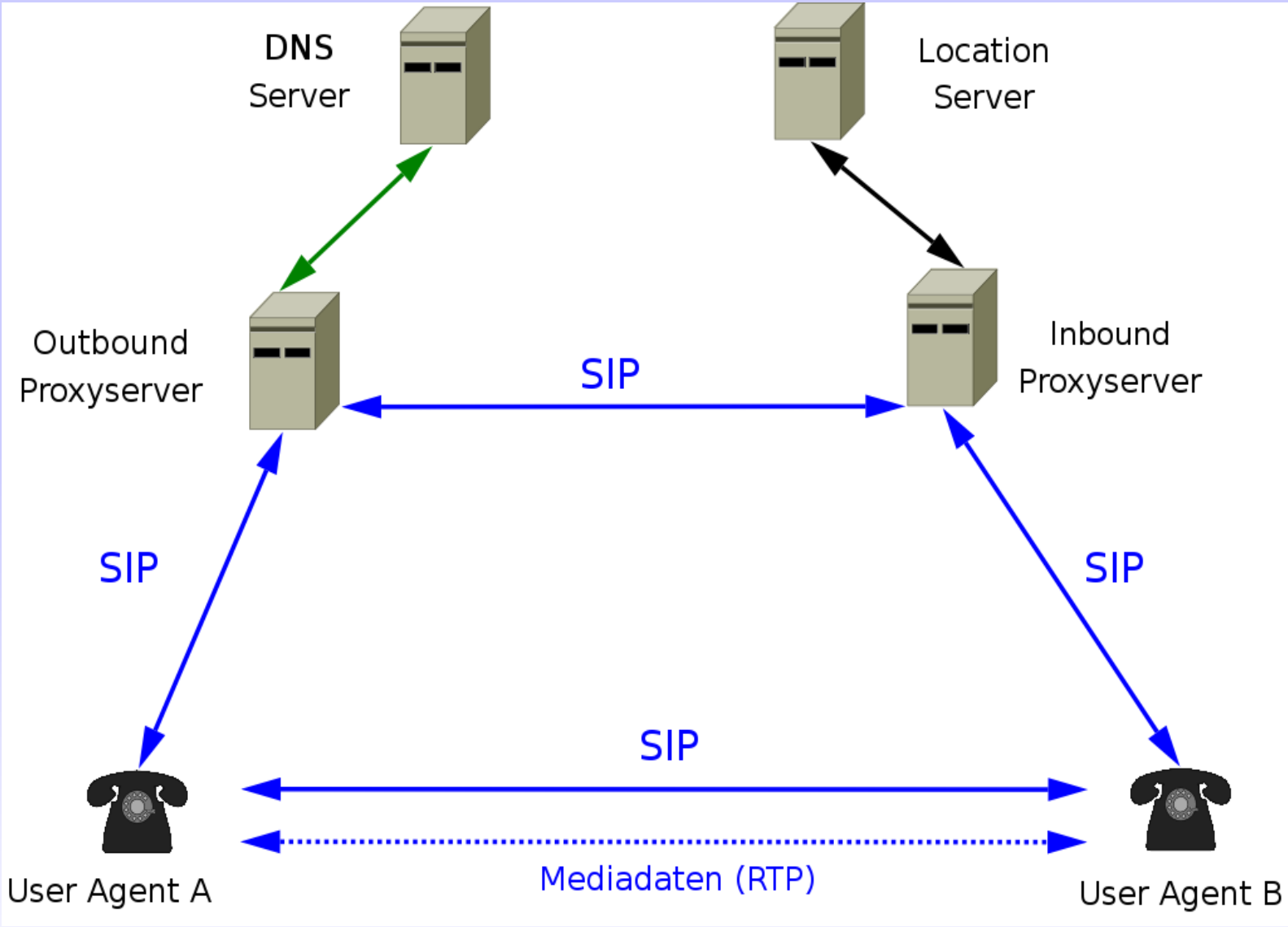
Digitale Telefonie

- Signalprotokolle
  - H.323 (Multimedia über LAN, jetzt auch Telefonie)
  - SIP (Sessionverwaltung für Video/Audio)
  - Beide seit 1996 in Existenz
  - Zusätzlich gibt es proprietäre Protokolle
- Mediadaten
  - Zoo von Audio-/Video Codecs

H.323 Komponenten



SIP Trapez


DNS
Server
Location
Server
Outbound
Proxyserver
SIP
Inbound
Proxyserver
SIP
SIP
SIP
User Agent A
Mediadaten (RTP)
User Agent B

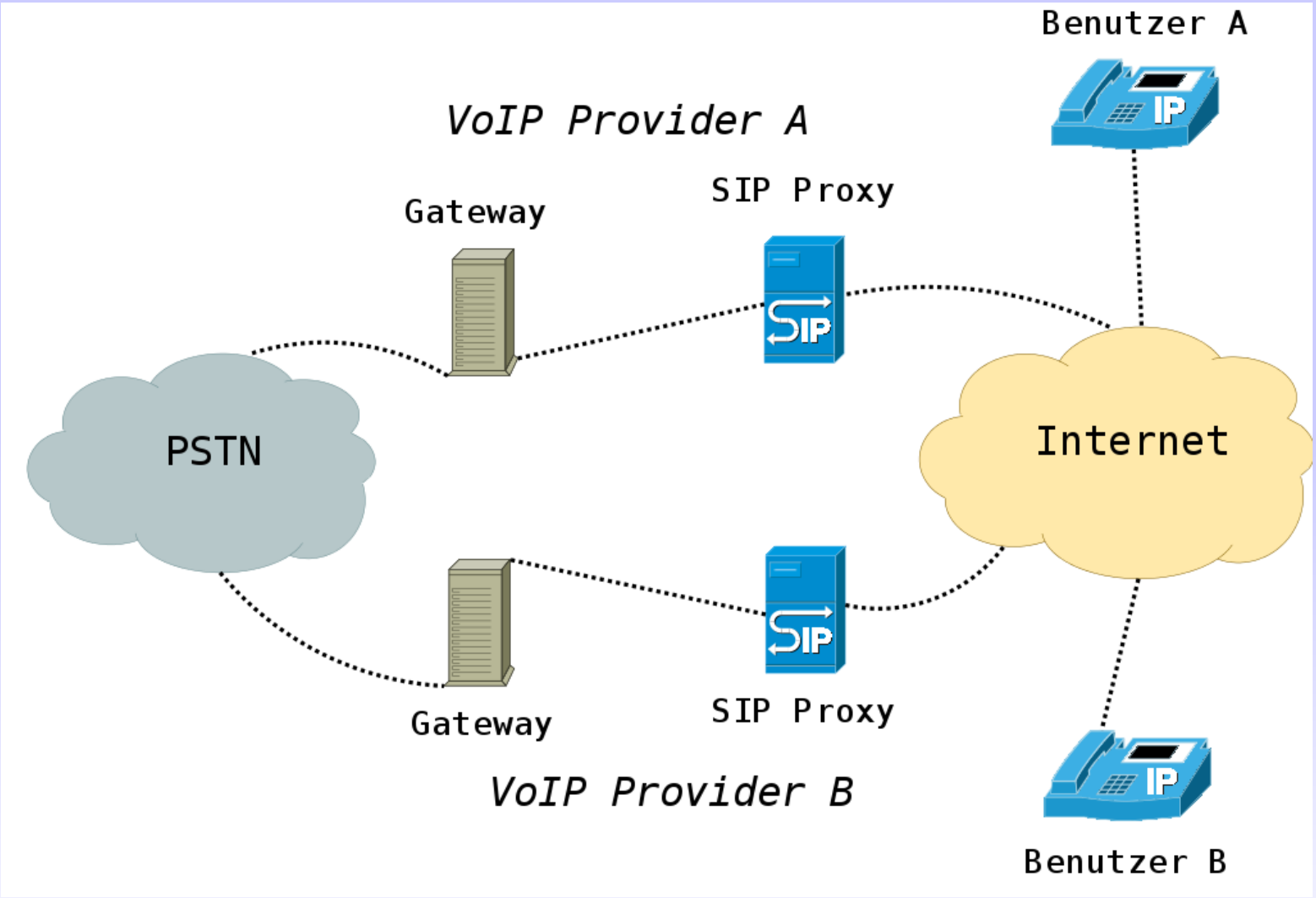
Voice over IT

- Digitale Telefonie breitet sich aus
- Nutzung bestehender IP Netzwerke
- Aus Telefonanlagen werden Server
  - IT “erbt” Telefonie
- Integration erweitert Anforderungen
  - Trotz Konvergenz Trennung von Daten/Telefonie
  - Zusätzliche Resourcen notwendig

Voice over IT Risiken

- VoIP konsolidiert Risiken
  - aus IP Netzwerken und
  - aus PSTN-/ISDN-/GSM-/GPRS-/UMTS-Netzwerken
  - “größter gemeinsamer Nenner”
- VoIP Telefone komplexer als analoge Verwandte
- VoIP bietet keine Vertraulichkeit
  - End-to-end Verschlüsselung beginnt erst
- VoIP Verfügbarkeit von IT abhängig

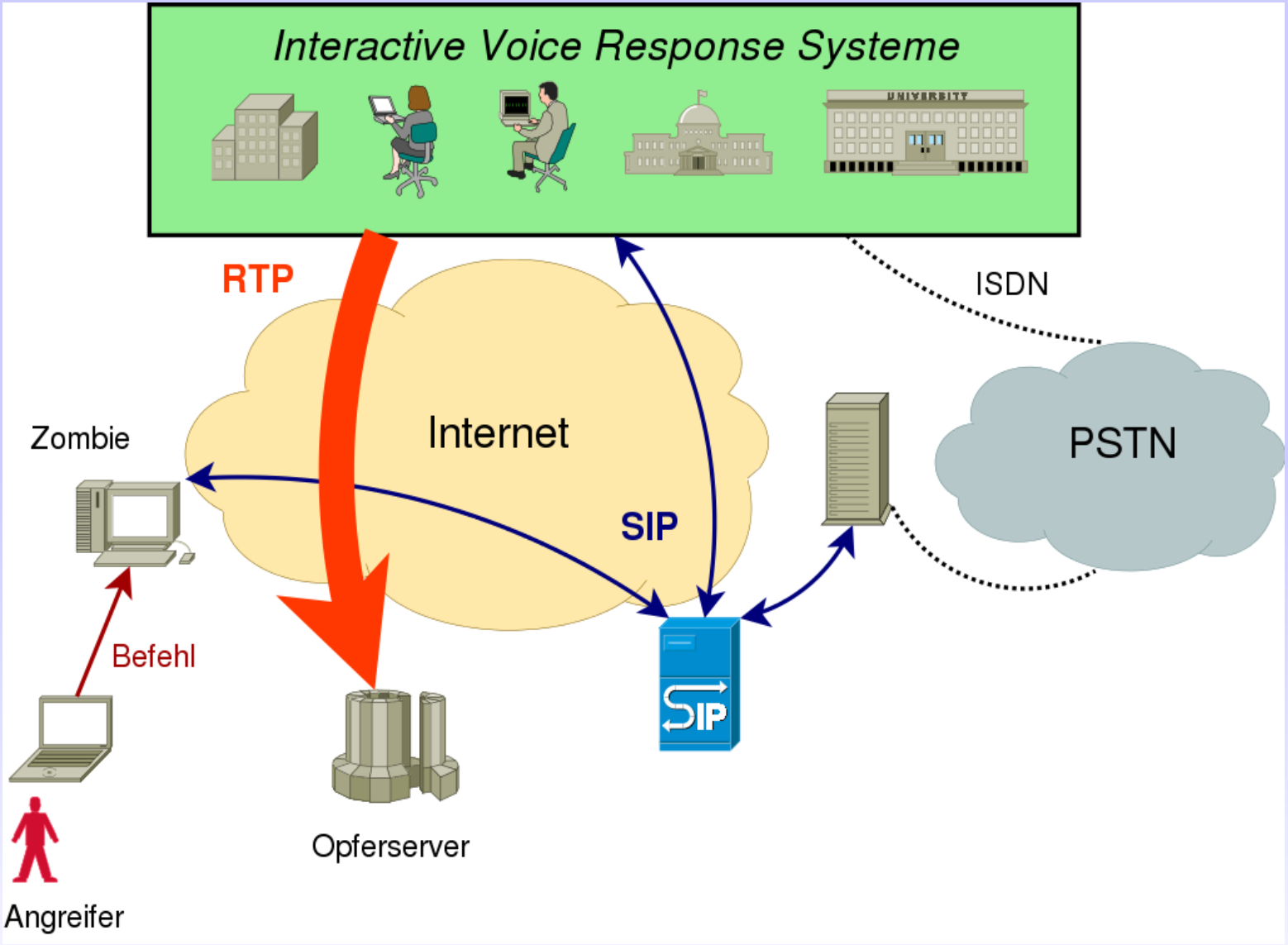
Vernetzung zwischen VoIP Anbietern



Erfahrungen aus IP Netzen

- Spam E-Mails
  - Mit VoIP und Software PBX realisierbar
- Phishing
  - Sprachmenüs mit Audiotexten leicht realisierbar
- (Distributed) Denial of Service
  - Gilt analog für digitale Telefonie
- IP Spoofing
  - Gilt für Caller ID, Registrierungen und (angreifende) Proxies
  - Umleiten von Anschlüssen

Telefone als Botnet



Traditionelle Gegenmaßnahmen

- Paketfilter und Content Inspection Proxies
- Serverhärtung (“Hardening”)
- Regelmäßige Überprüfungen der Konfiguration/Infrastruktur
- VPN zwischen Standorten und mobilen Clients
- Physisches LAN nur für Telefonie
- POTS- oder ISDN-Anschlüsse als Backup

IT Management

- Sicherheit bei Auswahl von Produkten beachten
  - Jeder Hersteller hat das “einzig wahre Produkt”
  - Spezifikationen beachten
  - Werbung ~~ignorieren~~ kritisch beleuchten
- VoIP Dienste sind auch nur Applikationen
  - ~~Chance~~ Change Management
  - Monitoring & Logging
  - Konfiguration(en) periodisch hinterfragen

Technologie täuscht

- Glauben Sie nicht alles!
  - Sind alle Ethernetkabel noch gleichlang?
  - Welches Subsystem benutzt welche Ports und VLANs?
  - Benutzt die Firma 7×24 den “richtigen” VoIP Anbieter?
  - Was passiert *wirklich* mit Telefonaten?
  - Schleusen Upgrades neue Hintertüren in die Systeme?
  - Gilt alles für Produktiv- und Backupsysteme gleich?
- Gibt es Prozesse, die periodisch solche Fragen stellen?
- Dürfen Mitarbeiter solche Fragen stellen?

Problem “Awareness”

- Umgang mit Software erfordert Schulungen
  - Teilweise in Prozesse und Personalwesen integriert
  - Weiterbildungen, Jobprofile
- VoIP erfindet Telefonie neu
  - Schulungen für Soft-/Hardphone
  - Schaffung von Awareness für *Sicherheit am Hörer* bzw. *Sicherheit am Mikrofon*

Umgang mit Telefonie

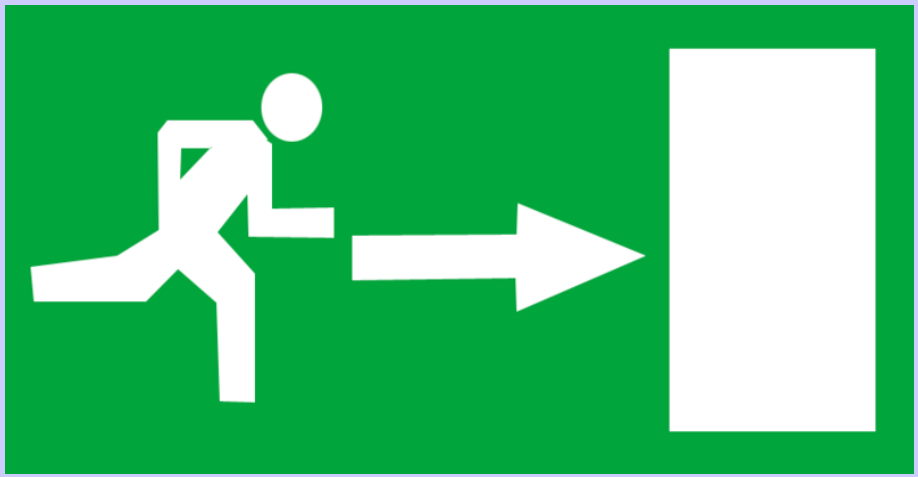
- Faktor Mensch ist wichtig
  - Kein ausschließlicher Fokus auf Technologie
  - Maßnahmen zur Absicherung noch zu unvollständig
- Richtlinien für Umgang mit Telefonie
  - Was darf besprochen werden?
  - Wo darf man telefonieren?
  - Welche Geräte darf man verwenden?

Zusammenfassung

- Sichere Telefonie analog sowie digital nicht möglich
- VoIP gruppiert Risiken nur anders
- VoIP Sicherheit steckt in Kinderschuhen
- Maßnahmen zur “best practice” Absicherung existieren
- Faktor Mensch spielt eine wesentliche Rolle
- IT wird formal zur ICT
  - Zusatz des Buchstabens C ersetzt kein Management!

Let us not look back in anger, nor forward in fear, but around in awareness.
-- *James Thurber*

Danke für Ihre Aufmerksamkeit!



Gibt es noch offene Fragen?

Über Consulting and Trainings (CaT)

- René Pfeiffer, selbständiger Berater
  - GSM +43 676 5626390, SIP +43 720 349387
- Michael Kafka, selbstständiger Trainer
  - GSM +43 664 4145905, POTS +43 1 8043144
- Dank an Dr. Christian Reiser, Paradigma Unternehmensberatung GmbH und Holger Schellhaas, Geschäftsführer der evoltas solutions ltd.

Voice over IT

Führt Konvergenz einer Technologie zu Divergenz beim Risiko?

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

Das Bild zeigt ein Feldtelefon der deutschen Bundeswehr aus dem Jahre 1980. Quelle: www.myinsulators.com

Worum es geht – der Überblick

- Informations-Telefonie (IT)
- Integration in “Infrakultur”
- Sicherheit und Risiken
- Anleitungen für Skeptiker
- Strategien zur Schadensbegrenzung

Begriff *Sicherheit*

- Begriff *Sicherheit* umfaßt bis Ende des Vortrags die
  - Integrität der Verbindungs-/Gesprächsdaten
  - Vertraulichkeit der Verbindungs-/Gesprächsdaten
  - Identität der Gesprächsteilnehmer
  - Verfügbarkeit der Infrastruktur

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

Der Begriff *Sicherheit* läßt sich verschieden definieren und hängt natürlich von den Anforderungen und Erwartungen ab. Sicherheit kann daher nur ein Kompromiß und kein absoluter Anspruch sein.

Bedrohungsszenarien

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

Das Gefahrenzeichen ist ein Warnzeichen nach DIN DIN 4844-2 und warnt vor nichtionisierender elektromagnetischer Strahlung.

Geschäftsmodell für Startups

a)Gründe Firma als VoIP Dienstleister

b)“Networking” mit anderen VoIP Firmen

c)“Modifizieren” von Geräten in deren Netzwerk

d)Dirigieren aller Anrufe über fremde Netze

e)Rechnungen für Dienste stellen, die andere bezahlen

“It's so easy a caveman can do it.”
-- Robert Moore, Techniker, verhaftet

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

Das Geschäftsmodell basiert auf einem wahren Fall. Ein VoIP Dienstleister aus Miami, Florida, hat sich Zugänge zu Netzwerken von 15 anderen VoIP Firmen verschafft und deren Netzwerke für das Führen der eigenen Kundengespräche benutzt. Die Rechnungen wurde ganz normal kalkuliert, aber andere Kosten als die Internet Standleitung fielen nicht an. Edwin Pena, der Geschäftsführer, wurde im Sommer 2006 verhaftet. Ihm drohen bis zu 25 Jahre Gefängnis und eine Strafe von bis zu 500.000$.

Artikel in der Informationweek
Interview mit einem Angestellten

Geschäftsmodell für Provider

- Telecom Italia
  “Prosecutors say the spy ring taped the phone conversations of politicians, industrialists and even footballers.” -- BBC Artikel (21.9.2006)
- Nutzen vorhandener Technik
  “According to Telecom Italia's own investigation, their procedure and machines used for the legal wiretaps had a number of flaws and it was technically possible to spy on the telephone conversations, without leaving any trace.” -- EDRi-Gram #4.15

Dieser Vorfall ging im Jahre 2006 weltweit durch die Presse und gesellt sich zu einer Reihe von Skandalen im italienischen Telekommunikationsbereich. Offenbar sind Gesprächsminuten von Politikern, Managern und Fußballstars Gold und Geld wert.

Geschäftsmodell für Unbekannte

- Ericsson entdeckt am 4. März 2005 trojanische Pferde im Lawful Interception Subsystem von Vodafon Greece.
- Kostas Tsalikidis, Leiter Network Design bei Vodafon Greece, erhängt sich am 9. März 2005
- Vodafon deaktiviert Subsystem und löscht versehentlich alle Logs und Spuren.
- Software im Subsystem hörte Telefonate von über 100 Regierungsmitgliedern ab.
- Täter sind unbekannt.
- Quelle: The Athens Affair (IEEE Spectrum, Juli 2007)

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

Telekommunikationsdienstleister müssen laut Gesetz in ihre Netzwerk Schnittstellen zum Abhören der Verbindungsdaten und der Gesprächsdaten einbauen. Diese Subsysteme für die sogenannte “Lawful Interception” sind standardisiert. Im Netzwerk von Vodafon Greece waren die Abhörschnittstellen schon aktiv (eingebracht durch einen Softwareupdate), aber die Systeme des Interception Management System (IMS) waren es noch nicht. Die Gespräche wurde durch Installation eines “rootkits” auf einem weiteren System und durch anschließende Umleitung der angezapften Verbindung auf 14-16 anonyme Wertkartentelefone abgehört.

Schlußfolgerungen aus Beispielen

Sicherheit und analoge Telefonie

- Endgeräte besitzen (kaum) Schutzmechanismen
- Telefonanlagen ebenso
- Zugang zu PSTN und Mobilnetzen beschränkt
  - “Geringe” Zahl von Providern
  - Authentisierung beschränkt auf Anschluß
  - GSM benutzt Smart Cards

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

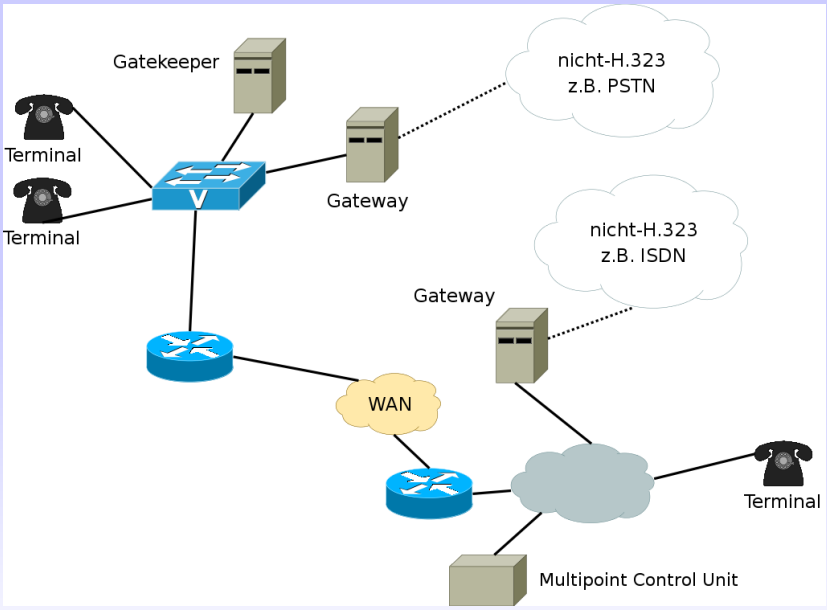
In diesem Vortrag sind Versuche zur Absicherung von Kommunikationswegen nicht erwähnt. Es gibt sehr wohl “sichere” Leitungen, Kryptofaxe und andere Zusätze. Alle Mittel sind jedoch nicht Teil des ursprünglichen Designs und wurden nachgerüstet. Diese Tradition sieht man auch im digitalen Bereich an der Entwicklung von Secure Socket Layer (SSL), auch bekannt als Transport Layer Security (TLS).

Digitale Telefonie

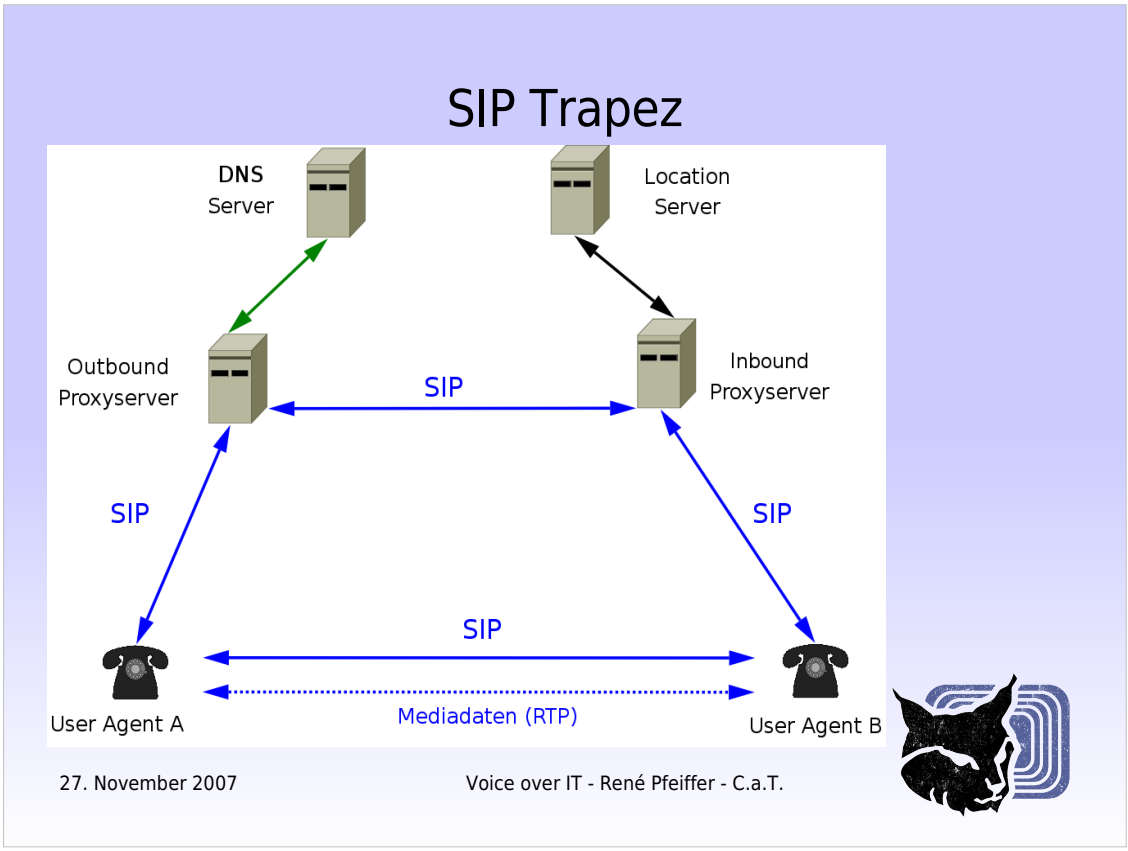
- Signalprotokolle
  - H.323 (Multimedia über LAN, jetzt auch Telefonie)
  - SIP (Sessionverwaltung für Video/Audio)
  - Beide seit 1996 in Existenz
  - Zusätzlich gibt es proprietäre Protokolle
- Mediadaten
  - Zoo von Audio-/Video Codecs

Die proprietären Protokolle wurden bewußt nicht betrachtet, um den Vortrag nicht in die Theorie abgleiten zu lassen und von Herstellern Abstand zu halten. Besagte Protokolle besitzen ähnliche Schwachstellen wie die offenen Standards. Bitte kontaktieren Sie die Autoren dieses Vortrags, um mehr Informationen zu erhalten oder im Einsatz befindliche proprietäre Protokolle zu überprüfen.

H.323 Komponenten



27. November 2007 Voice over IT - René Pfeiffer - C.a.T.


SIP Trapez
DNS
Server
Location
Server
Outbound
Proxyserver
SIP
Inbound
Proxyserver
SIP
SIP
SIP
User Agent A
Mediadaten (RTP)
User Agent B
27. November 2007
Voice over IT - René Pfeiffer - C.a.T.

Voice over IT

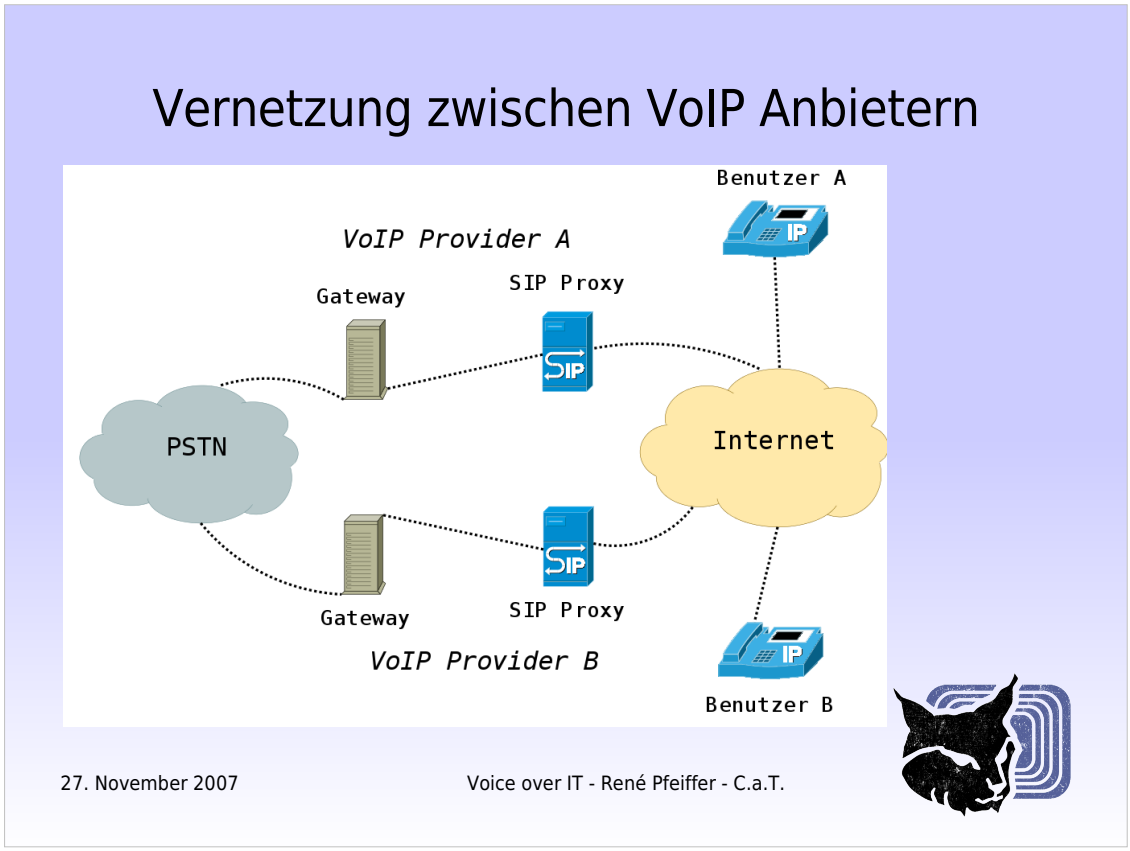
- Digitale Telefonie breitet sich aus
- Nutzung bestehender IP Netzwerke
- Aus Telefonanlagen werden Server
  - IT “erbt” Telefonie
- Integration erweitert Anforderungen
  - Trotz Konvergenz Trennung von Daten/Telefonie
  - Zusätzliche Resourcen notwendig

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

VoIP läßt sich nicht automatisch durch Installieren eines passenden Servers und Kauf passender Endgeräte implementieren. Man benötigt seperate Netzwerke mit Power over Ethernet (PoE), Quality of Service (QoS), abgeteilte/zusätzliche Standleitungen, Redundanzen und vieles mehr. Dadurch steigen die Kosten für eine komplette Umrüstung beträchtlich.

Voice over IT Risiken

- VoIP konsolidiert Risiken
  - aus IP Netzwerken und
  - aus PSTN-/ISDN-/GSM-/GPRS-/UMTS-Netzwerken
  - “größter gemeinsamer Nenner”
- VoIP Telefone komplexer als analoge Verwandte
- VoIP bietet keine Vertraulichkeit
  - End-to-end Verschlüsselung beginnt erst
- VoIP Verfügbarkeit von IT abhängig



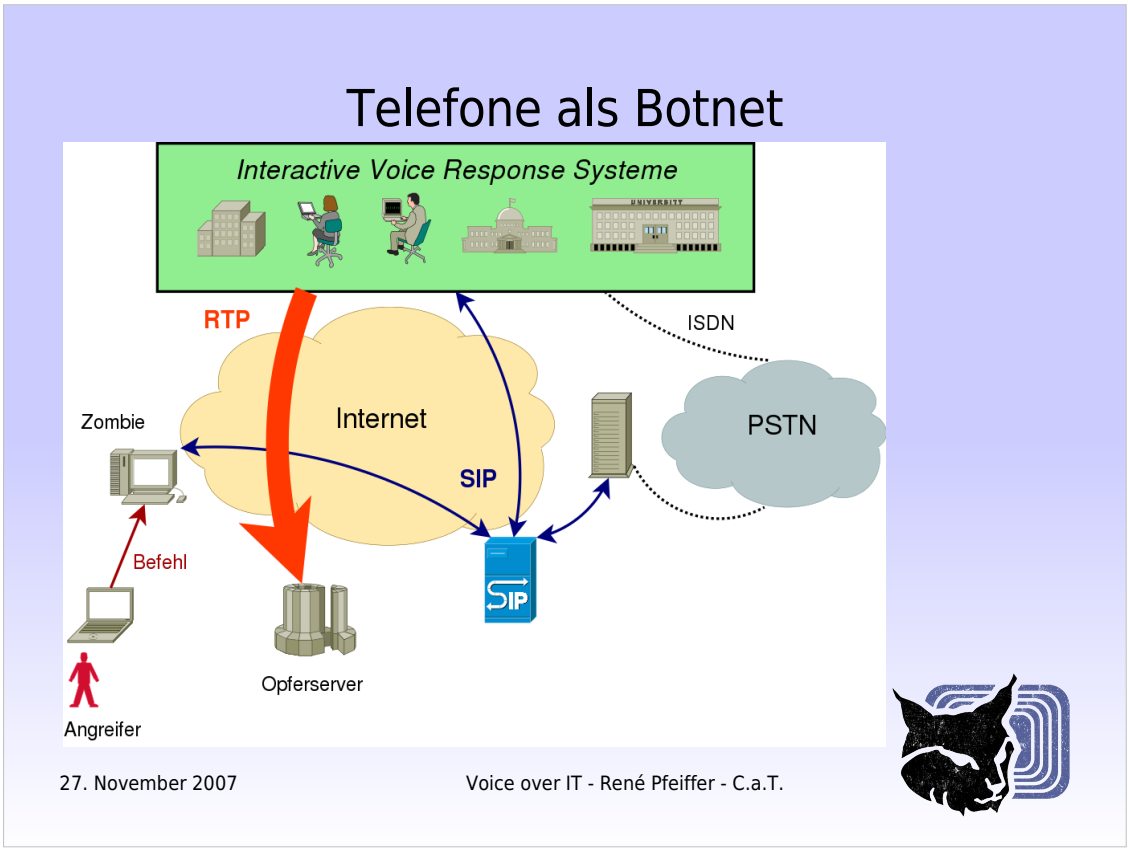
Es gibt zwar mittlerweile viele Anbieter von VoIP Diensten, aber die Vernetzung der “Telefonreiche” geschieht oft (noch) über das traditionelle Telefonnetz (PSTN). Im gezeigten Beispiel wäre die Abkürzung zwischen den beiden SIP Proxies denkbar, allerdings bedarf dies einer Abstimmung beider Firmen. Oft ist das Routing über analoge Netzwerke einfacher, da man dann kein explizites Vertrauensverhältnis zwischen den Firmen aufbauen muß. VoIP bedeutet daher nicht immer “100% digital”, und man muß solche Abhängigkeiten und Querverbindungen immer mit bedenken.

Erfahrungen aus IP Netzen

- Spam E-Mails
  - Mit VoIP und Software PBX realisierbar
- Phishing
  - Sprachmenüs mit Audiotexten leicht realisierbar
- (Distributed) Denial of Service
  - Gilt analog für digitale Telefonie
- IP Spoofing
  - Gilt für Caller ID, Registrierungen und (angreifende) Proxies
  - Umleiten von Anschlüssen

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

Die dargestellte Aufzählung von Risiken ist nicht vollständig und soll nur einen kleinen Einblick geben. Es fehlt beispielsweise *Spam over Internet Telephony* (SPIT), welches sehr leicht zu realisieren ist und Telefonie für Endbenutzer nachhaltig stören kann.



Interactive Voice Response (IVR) Systeme werden oft zur Benutzerführung bei Hotlines, Kartenbestellungen, Anrufbeantwortern oder anderen Diensten verwendet. Man kann IVR Systeme anrufen, und sie antworten in der Regel mit einem Audiostream. Das bedeutet, daß man mit wenigen SIP INVITE Pakten Telefonate aufbauen kann, die viele RTP Datenpakete erzeugen. Damit hat man einen klassischen Verstärker, der sich für DoS und DDoS Attacken eignet. Telefone und Telefonsysteme werden damit zu Bots in einem Botnet.

Quelle:

;login:, Ausgabe Oktober 2007, 32, Nummer 5

Traditionelle Gegenmaßnahmen

- Paketfilter und Content Inspection Proxies
- Serverhärtung (“Hardening”)
- Regelmäßige Überprüfungen der Konfiguration/Infrastruktur
- VPN zwischen Standorten und mobilen Clients
- Physisches LAN nur für Telefonie
- POTS- oder ISDN-Anschlüsse als Backup

Insbesondere bei Filtern stellt VoIP aufgrund der Real Time Daten eine Herausforderung dar. Es gibt enge Grenzen für die Überprüfung der Audiodaten, um Verzögerungen und Schwierigkeiten mit der Gesprächsqualität der Telefonate zu vermeiden.

IT Management

- Sicherheit bei Auswahl von Produkten beachten
  - Jeder Hersteller hat das “einzig wahre Produkt”
  - Spezifikationen beachten
  - Werbung ~~ignorieren~~ kritisch beleuchten
- VoIP Dienste sind auch nur Applikationen
  - ~~Chance~~ Change Management
  - Monitoring & Logging
  - Konfiguration(en) periodisch hinterfragen

Gerade Monitoring ist absolut wichtig und muß Bestandteil großer Netzwerke sein.

Technologie täuscht

- Glauben Sie nicht alles!
  - Sind alle Ethernetkabel noch gleichlang?
  - Welches Subsystem benutzt welche Ports und VLANs?
  - Benutzt die Firma 7×24 den “richtigen” VoIP Anbieter?
  - Was passiert *wirklich* mit Telefonaten?
  - Schleusen Upgrades neue Hintertüren in die Systeme?
  - Gilt alles für Produktiv- und Backupsysteme gleich?
- Gibt es Prozesse, die periodisch solche Fragen stellen?
- Dürfen Mitarbeiter solche Fragen stellen?

Problem “Awareness”

- Umgang mit Software erfordert Schulungen
  - Teilweise in Prozesse und Personalwesen integriert
  - Weiterbildungen, Jobprofile
- VoIP erfindet Telefonie neu
  - Schulungen für Soft-/Hardphone
  - Schaffung von Awareness für *Sicherheit am Hörer* bzw. *Sicherheit am Mikrofon*

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

Neue Technologien (oder alte in neuen Kleidern) führen immer Veränderungen herbei, die Benutzer sowie Systemadministration genau gleich treffen. Man muß Erfahrungen sammeln, vorsichtig sein und alle Maßnahmen periodisch überprüfen. Vielen ist die Komplexität von Telefonie nicht bewußt oder sogar unheimlich (analoge Telefonanlagen bekommen in der Regel weniger Beachtung als IP-vernetzte Systeme). Die Telefonie darf sich den Management Prozessen aber nicht entziehen.

Umgang mit Telefonie

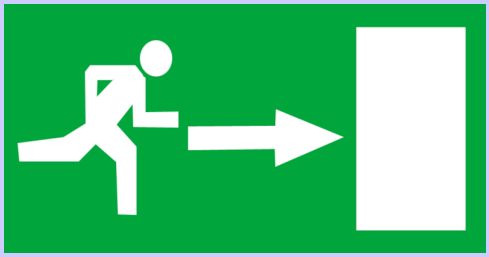
- Faktor Mensch ist wichtig
  - Kein ausschließlicher Fokus auf Technologie
  - Maßnahmen zur Absicherung noch zu unvollständig
- Richtlinien für Umgang mit Telefonie
  - Was darf besprochen werden?
  - Wo darf man telefonieren?
  - Welche Geräte darf man verwenden?

Zusammenfassung

- Sichere Telefonie analog sowie digital nicht möglich
- VoIP gruppiert Risiken nur anders
- VoIP Sicherheit steckt in Kinderschuhen
- Maßnahmen zur “best practice” Absicherung existieren
- Faktor Mensch spielt eine wesentliche Rolle
- IT wird formal zur ICT
  - Zusatz des Buchstabens C ersetzt kein Management!

Let us not look back in anger, nor forward in fear, but around in awareness.
-- *James Thurber*

Danke für Ihre Aufmerksamkeit!



Gibt es noch offene Fragen?

Über Consulting and Trainings (CaT)

- René Pfeiffer, selbständiger Berater
  - GSM +43 676 5626390, SIP +43 720 349387
- Michael Kafka, selbstständiger Trainer
  - GSM +43 664 4145905, POTS +43 1 8043144
- Dank an Dr. Christian Reiser, Paradigma Unternehmensberatung GmbH und Holger Schellhaas, Geschäftsführer der evoltas solutions ltd.

27. November 2007 Voice over IT - René Pfeiffer - C.a.T.

Bitte kontaktieren Sie uns, wenn Sie Interesse am vorgetragenen Thema haben. Wir beraten Sie gerne und helfen bei der Lösung bestehender oder bevorstehender Probleme. Sie können vom unserem Wissen auch bei einem der Workshops profitieren, die im Rahmen von Veranstaltungen angeboten werden. Individuelle Anfragen sind natürlich auch sehr willkommen!

http://web.luchs.at/
http://www.viennacircle.at/
http://www.paradigma.net/
http://www.evoltas-solutions.de/