LANCOM™ Techpaper: Sicherheit im Voice-over-IP-Umfeld

1 Sprachkommunikation im Computernetzwerk

Im Laufe der Geschichte haben technische Neuerungen immer wieder zu bedeutenden Veränderungen innerhalb der menschlichen Kommunikationsbeziehungen geführt. Neue Erfindungen boten die Möglichkeit zu völlig neuen Kommunikationsformen, die nicht selten entscheidenden Einfluss auf die gesamte Gesellschaft hatten.

In den letzten Jahren hat eine neue Kommunikationstechnologie zunehmend an Bedeutung gewonnen: Interaktive Netzwerke, die es dem Benutzer ermöglichen, große Informationsmengen zu senden oder zu empfangen. Das größte und am schnellsten wachsende interaktive Netzwerk ist das Internet. Noch vor wenigen Jahren beschränkte sich die Internetnutzung auf Wissenschaftler und Technologie-Fanatiker, aber die Zahl der Nutzer ist durch vereinfachte Zugangsbedingungen, günstigere und leistungsfähigere Computer und vor allem durch den wachsenden Informations- und Unterhaltungscharakter des Internet innerhalb kürzester Zeit stark gestiegen.

Durch die mittlerweile stark gewachsene Verfügbarkeit an breitbandigen Internetanschlüssen steht eine Innovation kurz vor ihrem Durchbruch, die alte und neue Kommunikationswege kombiniert und erneut entscheidenden Einfluss auf die gesamte Gesellschaft haben wird: die Internet-Telefonie.

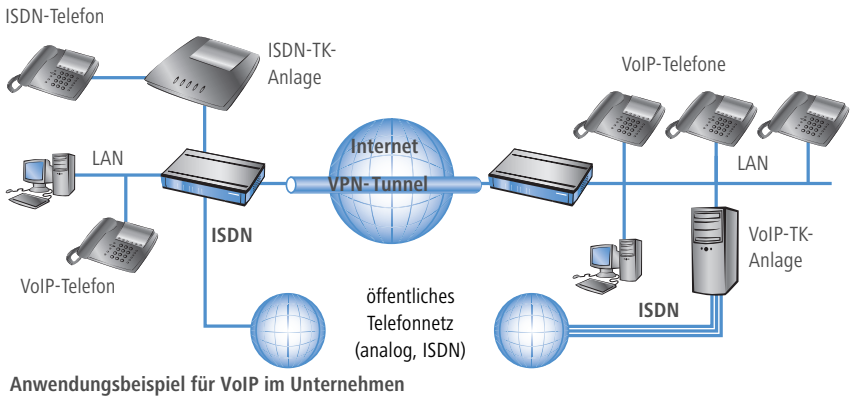
Kein Markt wächst derzeit so schnell und hat in der letzten Zeit für einen solchen „Hype" gesorgt wie der Bereich Voice over IP (VoIP). Steht für den Privatanwender vor allem die Reduzierung der Telefongebühren im Vordergrund, liegen die Kostenvorteile im Unternehmensbereich primär in den Synergieeffekten und der Konsolidierung der bestehenden TK- und IT-Infrastruktur auf das Ethernet.

Bei aller Freude über eine Technik, die einen erneuten Aufschwung in das angeschlagene IT- und TK-Umfeld bringen wird, sollte jedoch beachtet werden, dass für die Internet-Telefonie die gleichen Risiken gelten, die dem Anwender aus der IP-Welt bereits wohlbekannt sind. Daher ist das Thema Sicherheit von zentraler Bedeutung. Doch für die meisten Anwender steht derzeit nicht die Sicherheit von VoIP im Vordergrund, vielmehr sind sie noch damit beschäftigt, dass die Anrufe überhaupt zustande kommen.

Wie wichtig Sicherheit im Voice over IP-Umfeld – vor allem im Geschäftsverkehr – ist, zeigt sich daran, dass in letzter Zeit vermehrt Studien zu diesem Thema veröffentlicht wurden, zuletzt vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

2 Einsatzbereiche

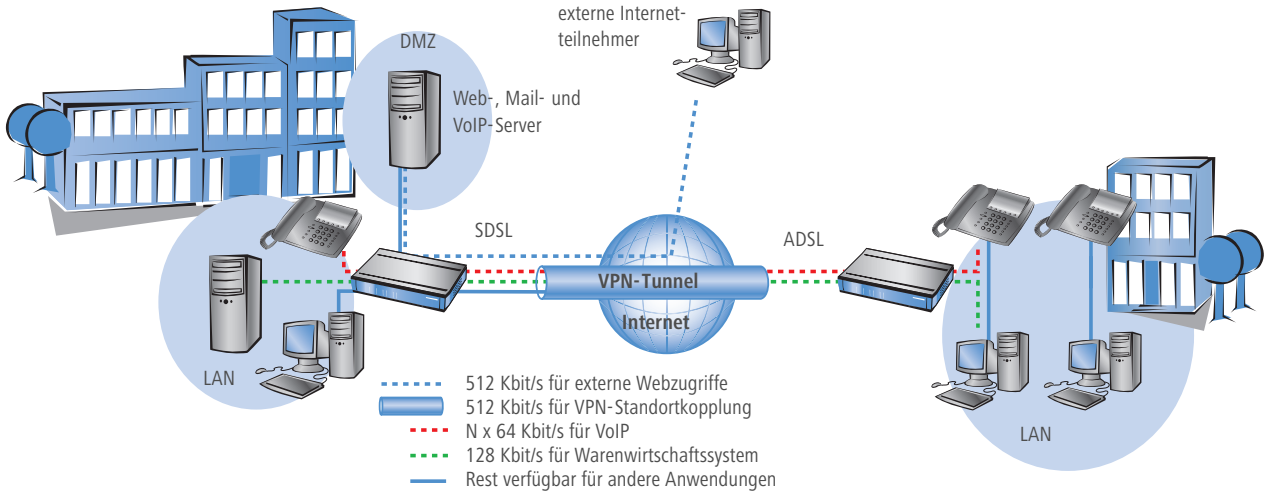
Im vorliegenden Dokument steht – wie auch in der Studie des BSI – VoIP-Telefonie im Vordergrund, die über Medien transportiert wird die vollständig im Verantwortungsbereich des Betreibers liegen. Nach bisherigen Erkenntnissen liegt der primäre Einsatzbereich von VoIP für Unternehmen in der Vereinfachung der internen Kommunikationswege und der Anbindung von Außenstellen oder Heimarbeitsplätzen an die unternehmenseigene TK-Infrastruktur. Die Kommunikation sollte hier auf jeden Fall über eine verschlüsselte VPN-Verbindung erfolgen. IP-Telefonate zwischen den einzelnen Standorten werden somit abhörsicher über den VPN-Tunnel übertragen. Der Datenstrom sollte an beiden Standorten über die Firewall geleitet werden, bevor er an das entsprechende VoIP-Endgerät weitergereicht wird.



Anwendungsbeispiel für VoIP im Unternehmen

LANCOM Systems

LANCOM™ Techpaper: Sicherheit im Voice-over-IP-Umfeld



Class of Service/Quality of Service für VoIP

3 Class of Service / Quality of Service

Neben klassischen Sicherheitsmaßnahmen wie strenge Regelwerke an den Firewalls, die öffentliches und privates Netzwerk trennen, Schutz vor Layer 2- und 3-Angriffen (z.B. ARP-, VLAN-, DHCP-, MAC-Angriffe, IP-Spoofing) und Abwehr von Denial of Service-Angriffen sollte für die Sprachübertragung eine so genannte Dienstegüte sichergestellt werden. Dies kann durch ein lückenloses Quality-of-Service-Management und die entsprechenden Regeln gewährleistet werden. Die eingesetzten VoIP-Geräte (Telefone, Router, TK-Anlagen) sind in der Regel in der Lage, dem Ethernet-Frame eines Sprachpakets eine Markierung gemäß DiffServ anzuhängen. Dadurch kann eine bevorzugte Weiterleitung der Sprachpakete realisiert werden, falls die eingesetzten Router in der Lage sind das Class of Service-Feld im Ethernet-Frame auszuwerten.

Eine logische Trennung von Sprach- und Datennetz kann durchgeführt werden, um – neben dem Management und der Skalierbarkeit – vor allem ein Quality of Service sicherzustellen. In Anbetracht aktueller Geschwindigkeiten von kabelgebundenen Netzwerken mit 100 Mbit bzw. 1 Gbit ist diese Absicherung aus Sicht der Dienstegüte nicht zwingend erforderlich, allerdings lässt sich damit die generelle Sicherheit erhöhen und die Beeinflussung der Sprache durch Datentransfers minimieren. Um auch höchsten Sicherheitsansprüchen gerecht zu werden, wie sie im Bereich der so genannten Verschlusssachenkommunikation vorgeschrieben sind, empfiehlt sich eine Authentifizierung aller Endgeräte (Daten und Sprache) nach 802.1x und eine statische MAC-Adress-Zuordnung pro Switch-Port. Derzeit existieren jedoch noch keine IP-Telefone, die explizit für die Verschlusssachen-Kommunikation freigegeben sind.

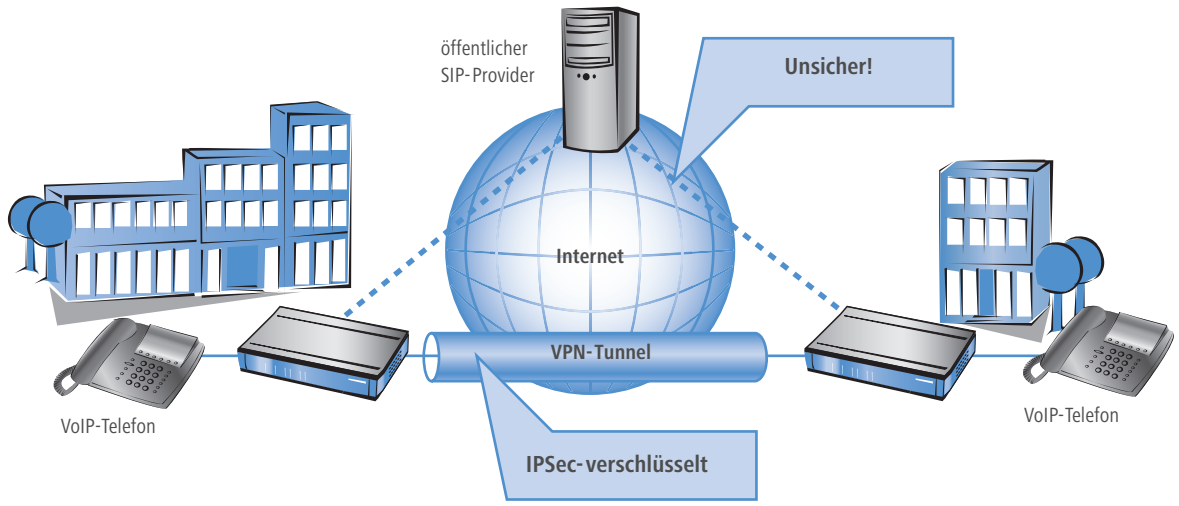
4 Verfügbarkeit

Die Verfügbarkeit des VoIP-Gateways muss zu jedem Zeitpunkt sichergestellt sein. Fällt die bestehende Internet-Verbindung aus, soll über geeignete Redundanzprotokolle (z.B. VRRP) auf ein Ersatz-Medium gewechselt werden können. Da die derzeitige Verfügbarkeit von DSL-Anschlüssen derzeit mit 97% angegeben ist (dies entspricht einem Ausfall von circa 11 Tagen) muss eine alternative Backup-Schnittstelle (z.B. ISDN oder UMTS) vorhanden sein, um den Betrieb der Datenkommunikation sicherstellen zu können. Alle aktuellen LANCOM Geräte mit dem „VoIP ready"-Logo sind zusätzlich in der Lage, die ISDN-Schnittstelle neben der Datenkommunikation auch noch für die Sprachvermittlung zu nutzen. Die Unterteilung erfolgt dabei auf B-Kanal-Ebene, d.h. ein Kanal kann weiterhin für den Datenverkehr genutzt werden und der zweite Kanal wird für den Sprachverkehr verwendet. Neben der telefonischen Erreichbarkeit der Mitarbeiter unter der bisher genutzten Rufnummer können so vor allem Notrufe und Ortsgespräche direkt in das öffentliche Telefonnetz ausgekoppelt werden.

Ferner sollte das Gateway eine „Lifeline"-Funktion beinhalten, die im Falle des Stromausfalls per Hardware-Relais den internen und externen ISDN-Anschluss durch-

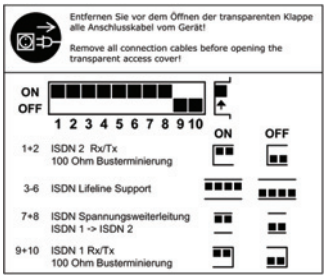
LANCOM Systems

LANCOM™ Techpaper: Sicherheit im Voice-over-IP-Umfeld



Einbindung eines SIP-Providers

schleift. Die Funktion der direkt an das Gateway angeschlossenen ISDN-Telefone wird dann mit der Phantomspeisung über den ISDN-Bus des Dienstanbieter sichergestellt.



Lifeline-Support beim LANCOM 1722 VoIP

5 Integration von SIP-Providern

Die meisten der erhältlichen VoIP-Gateways bieten die Möglichkeit, sich mit seinem Endgerät bei einem der großen SIP-Provider zu registrieren. Die im privaten Umfeld geschätzte Funktion bietet für den Geschäftskunden derzeit allerdings noch zwei große Nachteile:

1. Derzeit bieten nur wenige SIP-Provider eine mit dem ISDN-Anlagenanschluss vergleichbare Durchwahlmöglichkeit. Damit wird die Nutzbarkeit im Geschäftsbereich stark eingeschränkt.
2. Das SIP-Protokoll überträgt die Sprachdaten unverschlüsselt. Dadurch können auch technisch Unver-

Mitschnitt einer VoIPong-Session

```
efe:[voipong]# voipong -d4 -f
EnderUNIX VOIPONG Voice Over IP Sniffer starting...
Release 2.0-DEVEL, running on efe.dev.enderunix.org [FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE #0: Thu Dec i386]

(c) Murat Balaban http://www.enderunix.org/
19/11/04 13:32:10: EnderUNIX VOIPONG Voice Over IP Sniffer starting...
19/11/04 13:32:10: Release 2.0-DEVEL running on efe.dev.enderunix.org [FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE
#0: Thu Dec i386]. (c) Murat Balaban http://www.enderunix.org/ [pid: 71647]
19/11/04 13:32:10: fxp0 has been opened in  promisc mode, data link: 14 (192.168.0.0/255.255.255.248)
19/11/04 13:32:10:  [8434] VoIP call detected.
19/11/04 13:32:10:  [8434] 10.0.0.49:49606 <--> 10.0.0.90:49604
19/11/04 13:32:10:  [8434] Encoding: 0-PCMU-8KHz
19/11/04 13:38:37: [8434] maximum waiting time [10 sn] elapsed for this call, call might have been ended.
```


LANCOM Systems

LANCOM™ Techpaper: Sicherheit im Voice-over-IP-Umfeld

sierte Inhalte von geschäftskritischen Telefongesprächen mithören. Mit "VoIPong" steht ihnen hierfür ein mächtiges Werkzeug zur Verfügung, das in der Lage ist den Sprachanteil einer Datenverbindung zu extrahieren und für den Angreifer wieder hörbar zu machen. Solange keine verschlüsselten Protokolle wie SRTP und SIPS von den Providern angeboten werden, sollte daher Abstand von deren Integration genommen werden.

6 Anfoderungen an ein VoIP-Gateway

Zusammenfassend kann festgehalten werden, dass folgende Anforderungen an ein VoIP-Gateway gestellt werden müssen, um aktuellen Sicherheitsanforderungen an die Internet-Telefonie gerecht zu werden:

- Verfügbarkeit
  - Integrierte ISDN-Schnittstellen mit Lifeline-Support
  - Class / Quality of Service-Funktionen in Sende- und Empfangsrichtung
  - Sicherstellung der Hochverfügbarkeit über geeignete Protokolle und Kommunikationswege wie VRRP und ISDN
- Sicherheit
  - Schutzmechanismen wie Firewall und Denial of Service Protection
  - VPN-Funktionen für die sichere Sprachübertragung zwischen den Standorten
  - Unterstützung von logischen Netzen (VLAN)
  - Authentifizierungsmöglichkeiten von Endgeräten