Link: https://www.tecchannel.de/a/wege-zum-sicheren-voip,1742322

**Eine VoIP-Infrastruktur benötigt ein Sicherheitskonzept**

# Wege zum sicheren VoIP

Datum: 31.12.2007
Autor(en): Claudia Bardola

**Da VoIP die normale Netzwerk-Infrastruktur nutzt, weist sie auch dieselben Sicherheitsrisiken auf. Existierende (und künftige) Schwachstellen lassen sich aber auch leicht beheben.**

Lauschangriff, Gebührenbetrug oder Denial of Service: Peter Cox, Sicherheitsexperte aus England und Entwickler von **SIPtap**[1], ist nicht der Erste, der auf**die Gefahren der VoIP-Telefonie** [2] hinweist. Wenn also VoIP im Unternehmen als zentrales Kommunikationsmedium zum Einsatz kommen soll, ist es unabdingbar, die VoIP-Komponenten zuverlässig abzusichern.

Dieses Unterfangen ist allerdings nicht trivial und reichlich komplex. Bei klassischen Telefonanlagen reicht es häufig bereits, sie in ausreichend zugangsgeschützten Räumlichkeiten zu installieren. Dagegen ist bei der IP-Telefonie wesentlich mehr zu beachten:

VoIP ist durch alle von den IP-basierten und lokalen Netzen bekannten Mängel und Sicherheitsprobleme gefährdet: Beispiele sind Denial-of-Service-Attacken, Routing-Umlenkungen, Man-in-the-Middle-Angriffe oder das Abhören des Sprachverkehrs durch Sniffing. Dazu kommen auch noch Angriffe, die speziell die VoIP-Protokolle im Visier haben, wie etwa die Manipulation von Call-Routing-Tabellen.

Cyber-Kriminelle erhalten mit VoIP ganz neue Möglichkeiten: Für sie ist es ein Leichtes, die Absenderkennung zu verändern und das System für so genannten Spit (Spam over Internet-Telephony) oder Phishing zu missbrauchen. Hacker-Tools, mit denen sich VoIP-Systeme knacken lassen, sind inzwischen nicht nur in großer Vielfalt verfügbar. Sie lassen sich auch von technisch nur mittelmäßig versierten Angreifern nutzen, die so mit verhältnismäßig geringem Aufwand die entsprechenden Systeme manipulieren können.

Eine aus der IT-Welt bekannte Methode ist beispielsweise das Pharming: Die Gespräche werden über einen Fremdserver geleitet – gänzlich unbemerkt vom Benutzer. Die Hacker können die Telefonate abhören oder SIP-Passwörter abfangen.

## 1. Die Risiken unter Kontrolle

Doch ebenso wie die Hacker und Betrüger auf aus der IT-Landschaft bekannte Tools zurückgreifen können, stehen auch den VoIP-Anwendern gleichsam bewährte Gegenmittel zur Verfügung. Denn letztlich ist VoIP ja nicht mehr, als eine weitere IT-Applikation. Die damit verbundenen Risiken sind größtenteils bekannt und entsprechend gut in den Griff zu bekommen.

Dennoch muss, damit eine VoIP-Infrastruktur zuverlässig geschützt werden kann, ein umfassendes Sicherheitskonzept erstellt werden, welches sämtliche Komponenten des Systems berücksichtigt.

Den Grundstein eines solchen Konzepts stellt - wie bei klassischen TK-Anlagen auch - die **physische Absicherung aller beteiligten Systemkomponenten** dar. Diese dürfen ausschließlich für autorisierte Administratoren zugänglich sein.

Zweite Säule der VoIP-Absicherung ist die **Abschottung des Netzes**. Um Manipulationen am und über das Netz einen Riegel vorzuschieben, gibt es unterschiedliche Varianten: So können das Sprach- und Datennetz wahlweise durch ein VLAN oder durch die Verwendung unterschiedlicher Ports voneinander getrennt werden.

Zur **Absicherung der Wege**, auf denen die Sprachdaten transportiert werden, empfiehlt sich der Einsatz eines VPN (Virtual Private Network). Hierbei wird die sichere Datenkommunikation zwischen mehreren Standorten eines Unternehmens gewährleistet, indem der gesamte Datenverkehr auf fest definierten Verkehrswegen und über zuverlässig überwachte Router geleitet wird.

# 2. Verschlüsselung und Endgeräte

Die VPN-Technik sichert allerdings nur den Übertragungsweg der Sprachdaten. Zur Sicherstellung einer umfassenden End-to-End-Security sind daher noch weitere Schritte nötig. So müssen einerseits die Sprachdaten verschlüsselt werden. Andererseits ist dafür zu sorgen, dass auch die entsprechenden Signalisierungsdaten verschlüsselt werden.

Dies trifft insbesondere auf das allgegenwärtige SIP (Session Initiation Protocol) zu. Letzteres ist für die Session-Kontrolle zuständig, also beispielsweise die Registrierung der Endgeräte, den Rufaufbau und den Rufabbau. Wenn SIP im Einsatz steht, tauschen die Endgeräte verschiedene Nachrichten miteinander und mit den Applikationsservern aus. Weil die SIP-Nachrichten aber textbasiert und meist als Klartext gesendet werden, könnten sie leicht abgefangen, gefälscht und manipuliert werden.

Weiterer Handlungsbedarf besteht bei der Codierung des Administrationsverkehrs: VoIP-Komponenten lassen sich über verschiedene Protokolle wie HTTP, Telnet, SSH oder HTTPS administrieren, von denen einige die Benutzer- und Passwortdaten ebenfalls als Klartext übertragen, also sehr leicht abhörbar sind. Für eine sichere Verwaltung der VoIP-Komponenten müssen die administrativen Verbindungen entweder verschlüsselt werden oder über einen gesonderten Netzbereich erfolgen.

Überdies müssen alle Endgeräte wie VoIP-Telefone und Softphones am PC in das Sicherheitskonzept miteinbezogen werden. Denn VoIP-Endgeräte können durch Manipulationen der Konfigurationen oder der Firmware das gesamte Netz in die Knie zwingen. Dies lässt sich verhindern, indem Änderungen an der Konfiguration nur zentral über eine Applikation an einzelnen Geräten oder an Gerätegruppen erlaubt sind.

# 3. Risikofaktor Mensch

Weil die Mitarbeiter bekanntermaßen das größte Sicherheitsrisiko in der IT darstellen, reichen die erwähnten technischen Maßnahmen zur umfassenden Absicherung eines VoIP-Systems nicht aus.

Zumal gerade bei VoIP die Gefahren durch die Anwender noch größer sind als bei klassischen IT-Applikationen. Dies vor allem deshalb, weil bei VoIP zusätzliche Anwendungen betroffen sind: So bietet ein ungesperrtes Telefon Einblick in Ruflisten, Voice-Mails und Telefonbücher.

Ein Angreifer kann an einem ungesicherten Gerät die Sprachverschlüsselung deaktivieren und die Gespräche auf seinen Rechner umleiten. Deshalb ist es wichtig, die Mitarbeiter im Rahmen einer ausführlichen Schulung für den sicheren Umgang mit VoIP zu sensibilisieren. Zudem sollten umfassende Security-Regeln aufgestellt werden.

# 4. Vorsicht ist besser als Nachsicht

In den vergangenen Jahren spielte das Thema Security bei VoIP-Einführungen eine eher untergeordnete Rolle. Dies ist hauptsächlich darauf zurückzuführen, dass bislang nur wenige Angriffe auf VoIP-Systeme öffentlich bekannt wurden. Unternehmen dürfen sich deshalb aber nicht in falscher Sicherheit wiegen. Einem aktuellen Bericht der Security-Experten von **McAfee**[3] zufolge hat sich dieses Jahr die Zahl der VoIP-Sicherheitslücken gegenüber dem Vorjahr mehr als verdoppelt. McAfee geht für 2008 von einer weiteren Zunahme der VoIP-Risiken um bis zu 50 Prozent aus.

Daher gilt: Unternehmen können durch VoIP zwar personelle Ressourcen für die Betreuung der Telefonie-Infrastruktur einsparen. Gleichzeitig muss aber in die IT-Abteilung investiert werden, um die VoIP-Infrastruktur optimal absichern zu können. Und zwar sowohl in personeller wie auch in materieller Hinsicht. (**Computer World**[4]/mha)

# 5. Checkliste

Mit diesen Vorkehrungen wird VoIP sicherer:

- Daten und Sprache müssen im Netz logisch voneinander getrennt werden;
- Sprach- und Signalisationsdaten sowie der adminstrative Verkehr sind zu verschlüsseln;
- es müssen starke Zugangskontroll- und Authentifizierungssysteme installiert sein;
- die Standard-Passwörter sind für VoIP-Anlagen und VoIP-Endgeräte zu ändern;
- Neue Patches für das System müssen sofort eingespielt werden;
- Die Mitarbeiter müssen für die Gefahren von VoIP sensibilisiert werden.

Dieser Artikel stammt von unserer Schwesterpublikation der **Computerworld Schweiz**[5].

## Links im Artikel:

[1] **http://siptap.voipcode.org/**
[2] **https://www.tecchannel.de/link.cfm?pk=432698**
[3] **http://www.mcafee.com/**
[4] **http://www.computerworld.ch/**
[5] **http://www.computerworld.ch/**

---