Voice over IP (VoIP) gehört in den letzten Jahren zu den wichtigsten Entwicklungen innerhalb der Informationstechnolgie.

Sicherheitsaspekte bei Voice over IP

Von Dr. Ivan Roman

VoIP bietet sehr viele Möglichkeiten und Vorteile an. Bei Privatpersonen stehen oft kostenlose Gespräche zwischen VoIP-Nutzern und günstige Angebote für den Zugang in die klassischen Telefonienetze im Vordergrund. Bei Firmen ist die Integration von Daten- und Sprachkommunikation und die Reduktion der Betriebskosten sehr interessant. Das Zusammenfliessen verschiedener Kommunikationsformen wird weiter gehen und das Thema der Zukunft in der Telekommunikation wird "Konvergenz" heissen.

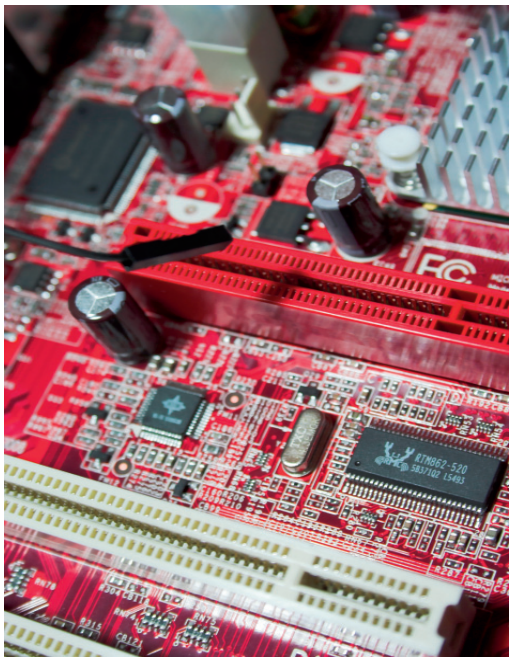

Foto:pc-freak

Bei der ganzen Begeisterung besteht jedoch die Gefahr, dass man im Hype die Sicherheitsproblematik ausser Acht lässt.

Gefahren

Bei VoIP handelt es sich um eine IP-basierende Technologie. Man verlässt also die gewohnte, anscheinend völlig sichere Umgebung der traditionellen Telefonie und steigt in die "böse" Viren-, Hacker- usw. gefährdete IP-Welt ein. Dementsprechend ist VoIP primär den gleichen Gefahren ausgesetzt, wie die übliche IP-Infrastruktur. Zusätzlich kommen noch einige VoIP-spezifische Gefährdungen dazu.

Zur Sicherstellung der IT-Sicherheit geht man in der Regel von drei Grundanforderungen aus :

- Verfügbarkeit (Ist die Verfügbarkeit eines Dienstes oder Systems gewährleistet ?)
- Vertraulichkeit (Ist der Verkehr vor unberechtigtem Mitlesen/Mithören geschützt ?)
- Integrität (Kommen die Daten unverfälscht am Zielort an ?)

Diese Methode lässt sich auch für die Betrachtung der VoIP-Sicherheit anwenden.

Verfügbarkeit

Die Verfügbarkeit ist ein sehr wichtiger Aspekt, der unser Interesse verdient. Eine nicht funktionierende Telefoninfrastruktur kann enorme wirtschaftliche Einbussen und auch Imageschäden nach sich ziehen.

Die klassische Telefontechnologie verfügt über eine hohe Verfügbarkeit. Entsprechend erwarten die Anwender, dass

VoIP eine ähnliche Verfügbarkeit aufweist. Eine Erklärung im Sinne "Das System wird gerade gebootet", welche im IT-Umfeld evtl. noch eine bestimmte Akzeptanz hat, wird beim Sprachdienst mit Recht nicht toleriert. Ein System-Ausfall kann sowohl absichtlich als auch unabsichtlich erfolgen. Bei einem unbeabsichtigten Stromausfall funktioniert die IP- und hiermit auch VoIP-Infrastruktur, wenn man keine Vorkehrungen getroffen hat, nicht mehr.

Die Verfügbarkeit kann auch absichtlich beeinträchtigt werden. Solche Angriffe werden als DOS (Denial-of-Service)-Angriffe bezeichnet.

Es gibt eine ganze Reihe von DOS-Angriffen:

DOS-Angriffe auf VoIP-Systeme

Bei den VoIP-Systemen (Endgeräte, Server, Switches, ...) handelt es sich um klassische IT-Systeme und als solche den klassischen DOS-Angriffen (z.B. "Buffer Overflow", Überflutung,...) ausgesetzt.

DOS-Angriffe auf den Signalisations- respektive Datenpfad

Das SIP-Protokoll verwendet verschiedene Befehle (z.B. CANCEL, BYE) und Antwort-Codes, welche sich für einen DOS-Angriff missbrauchen lassen (z.B. Sitzungsabbruch).

Ähnliche Resultate erzielt man mit dem Einfügen von Daten mit hohen RTP-Nummern im Datenpfad.

Bei der Verfügbarkeit ist auch der Aspekt der "Notfallnummern" sehr wichtig: Sanität, Polizei, Feuerwehr, ... müssen immer erreichbar sein! Dabei spielt die Lokalisierung des Anrufers eine wichtige Rolle. VoIP bietet die Möglichkeit, von überall auf der Welt mit der gleichen Nummer zu telefonieren. Aufgrund der Nummer allein lässt sich dann der Aufenthaltsort der telefonierenden Person nicht feststellen. Genau das ist aber für die Alarmierung der Rettungsdienste entscheidend.

Vertraulichkeit

Die Lauschangriffe gehören zu den klassischen Angriffstypen. Bei den VoIP-Verfahren wie Session Initiation Protocol (SIP), H.323 oder Skinny Client Control Protocol ist dies sehr gut möglich. Sie definieren zwar verschiedene Signalisierungs-Protokolle, für den eigentlichen Sprachtransport setzen sie meistens das RTP (Real-Time Transport Protocol) ein. Der RTP-Datenstrom ist standardmässig unverschlüsselt. Mit den im Internet frei verfügbaren Werkzeugen lassen sich die RTP-Pakete mitschneiden, als Audiodatei abspeichern und später abspielen. Der Hakker kann solche Daten an einem Hub mitlesen, resp. durch Modifikation der ARP-Tabellen den Verkehr auch im Switch-Umfeld entsprechend umleiten. Als Bedrohungsszenarien kann man sich beispielsweise das Abhören einer PIN-Abfrage, oder eines vertraulichen Arztgespräches etc. vorstellen.

Abwehrmassnahmen

Schützen Sie Ihre Daten gegen Lauschangriffe und Verfälschungen!

- Klären Sie bei den verschiedenen VoIP-Lösungen, ob und wie die Verschlüsselung und Integritätskontrollen implementiert sind. Konfigurieren Sie Ihre Systeme entsprechend.
- Schützen Sie Ihre VoIP-Infrastruktur gegen DOS-Angriffe!
- Ihre VoIP-Systeme müssen geschützt werden! Setzen Sie starke Antivirus-Lösungen ein, "patchen" Sie die Systeme gegen Buffer-Overflow und andere DOS-Angriffe. Setzen Sie starke Authentifizierungsmethoden ein!
- Kontrollieren Sie die VoIP-Verfügbarkeit inkl. Erreichbarkeit der Notfallnummern!
- Bereiten Sie den möglichen Fall des Stromausfalls vor! Sorgen Sie für eine Notstromversorgung! Bereiten Sie einen Backup-Telefondienst vor!
- Klären Sie den Einsatz von Firewalls und NAT detailliert ab!
- Die klassischen Firewalls und NAT wurden für den Schutz von Datennetzwerken entwickelt. VoIP stellt an die Firewalls allgemein und an NAT im Speziellen diverse neue Anforderungen! Klären Sie deren Einsatz ab!
- Training und Sensibilisierung der Anwender. Anwender müssen die VoIP-Gefahren kennen. Sie müssen geschult werden, wie sie ihre VoIP-Systeme zuverlässig und sicher einsetzen.

Schlussfolgerungen

VoIP ist eine zukunftsträchtige Technologie und nimmt an Bedeutung immer mehr zu. Die VoIP-Sicherheitsaspekte sollten aber von Anfang an, bei der Planung, bei der Evaluation, bei der Konfiguration und im Betrieb ernst genommen werden.

Dr. Ivan Roman, Consultant und Trainer bei der IT-Security Weiterbildungsfirma Roman-Consulting & Engineering AG in Zürich, www.roman.ch