Neue Gefahren mit VoIP

Voice over IP ist zu einem ständigen Begleiter geworden. Überall liest und hört man von der neuen kostengünstigen Technik mit den vielen Möglichkeiten. Doch mit der neuen Errungenschaft kommen auch neue Gefahren auf uns zu.

Bis 2008 werden über 90 Prozent aller neuen Telefonzentralen auf Voice over IP basieren. So hat es die Gartner in einer Studie veröffentlich. Diese Erwartungen wurden zwar nicht erfüllt, zeigen aber, dass dies zu einem Dauerthema geworden ist. Eine solche Verbreitung zieht natürlich auch die Hacker und Cracker magisch an. Grund genug, sich auch mit den Gefahren und Risiken auseinanderzusetzen.

Eine wichtige Organisation zur Identifikation von Gefahrenquellen ist dabei die Voipsa (Voice over IP Security Alliance), zu welcher über 100 Provider, Hard- und Softwarehersteller angehören. In der aktuellen Studie «Threat Taxonomy» wurden über 60 Gefahrenpotenziale für VoIP-Netze, -Endgeräte und -Anwender umfassend beschrieben.

Die genannten Gefahren teilen sich in

- Soziale Angriffe,
- Lauschangriffe,
- Gesprächskontrolle und
- Störungen auf.

ZUM AUTOR

Dipl.-Ing, FH, CISSP, Andreas Wisler
IT-Redaktor Maschinenbau
Geschäftsführer GO OUT
Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 320 91 20
www.goout.ch
info@goout.ch

Soziale Angriffe

Diese Art von Angriffen zielt auf die Persönlichkeit einer Person. Es wird versucht, möglichst viele Informationen über die Person zu erfahren, um anschliessend diese Identität zu übernehmen. Viele Provider von VoIP-Diensten erleichtern dies, indem die eigene Rufnummer, die so genannte Caller ID, relativ einfach gefälscht werden kann. Damit ist es möglich, eine x-beliebige Nummer zu übernehmen, die beim Angerufenen auf dem Display erscheint und so Vertrauen erweckt. Erschwerend kommt hinzu, dass viele Anbieter die unterdrückte Rufnummer trotzdem mitschicken. Angezeigt wird diese im Display zwar nicht, aber mittels einer Protokollanalyse sind alle Angaben sichtbar. Bei Anrufen auf Notfallnummern macht dies zwar Sinn, jedoch sollte die unterdrückte Nummer nicht bei allen Anrufen mitgeschickt werden.

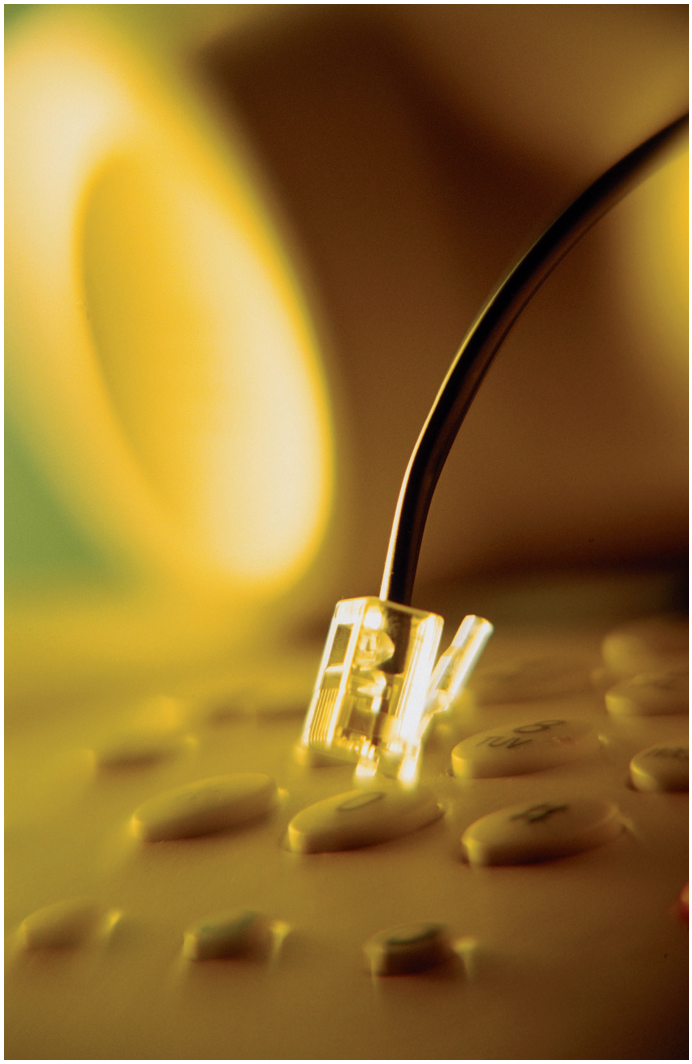

Bild: Archiv

Mit den gestohlenen Identitäten wird bereits heute im Internet gehandelt. Vor allem für Scheinverkäufe bei Ebay herrscht ein reger Handel mit diesen Angaben.

Ein weiterer Faktor sind Spam-Meldungen. Wie bei Email bereits unrühmlich bekannt, nimmt auch Spam über VoIP schnell zu.

Für den Versender solcher Werbemitteilungen sind keine oder nur marginale Kosten verbunden, der Empfänger hingegen muss sich eine gesprochene Mitteilung anhören. Daher gilt, wie bei Emailadressen, nur vertrauenswürdigen Personen und Institutionen die eigene Rufnummer bekannt geben.

Skype

Das kostenlose Programm Skype hat Voice over IP erst bekannt gemacht. Durch die einfache Installation und Benutzung hat sich eine riesige Anwender- und Fangruppe gebildet. Immer wieder wird über die Sicherheit dieser Applikation diskutiert. Da der Programmcode nicht öffentlich bekannt ist, kann auch kein abschliessendes Urteil gebildet werden. Fakt ist jedoch, dass viele Angriffe auf typische Voice-over-IP-Geräte bei Skype nicht möglich sind. Zusätzlich werden die Verbindungen zwischen Anrufer und Angerufenen mit AES sicher verschlüsselt. Ein Abhören ist somit nicht ohne weiteres möglich.

Lauschangriffe

Lauschangriffe sind eine klassische Methode, die aus vielen Filmen bekannt ist. Auch bei digitalen Nachrichten wird versucht, den gesprochenen Text mitzuhören. Dazu müssen jedoch die Datenpakete abgefangen und zusammengesetzt werden. Auf dem Internet sind bereits zahlreiche Tools verfügbar, die diese Arbeit automatisch übernehmen. Jedoch kann nicht einfach ein Kabel «angezapft» werden, sondern die Pakete müssen über den eigenen Rechner umgeleitet werden. «Man in the middle Attacken» nennt man diese Möglichkeit. Damit dies erst möglich wird, muss der Benutzer dazu gebracht werden, eine Software einzuspielen. Hier kommt wieder der soziale Faktor dazu. Gelingt es, dem Benutzer eine Software unterzujubeln (dies können zum Beispiel Viren, Trojanische Pferde oder eine Email mit «Beilage» sein), werden alle Pakete zuerst an den Angreifer geschickt und erst dann weiter an den eigentlichen Empfänger.

Gesprächskontrolle

Gelingt es, eine Verbindung so zu übernehmen, sind nebst dem Abhören auch Manipulationen am Gespräch möglich, so zum Beispiel das Verändern von Inhalten, Rufumleitungen oder dem Beenden des Gespräches.

Störungen

Anders als bei der bekannten Telefonie, können Voice-over-IP-Geräte mit relativ kleinem Aufwand gestört werden. Zu den bekanntesten Angriffen zählen DoS-Angriffe (Denial of Service). Das Ziel ist es, die Infrastruktur so zu «beschäftigen», dass ein normaler Betrieb nicht mehr möglich ist. Wahlwiese werden so viele Datenpakete an den Empfänger geschickt, dass die Leitung überlastet oder es wird eine Schwachstelle im Endgerät ausgenutzt, welche das Gerät zum Absturz bringt. In der Folge können weder Telefonate empfangen noch gemacht werden. Wie bei DoS-Angriffen auf eine Webseite, ist ein Schutz der VoIP-Infrastruktur nur sehr schwer möglich.

Schutzmöglichkeiten

Dass die oben beschriebenen Gefahren real sind, zeigen die verschiedenen Tools und Anleitungen, die im Internet abrufbar sind. Schutzmöglichkeiten umzusetzen ist jedoch nicht einfach. Nicht alle Hersteller implementieren die Standard-VoIP-Protokolle in der gleichen Art und Weise. Ein effektiver Schutz kann im Moment nur bei den Herstellern geschehen. Sie müssen Möglichkeiten implementieren, die weder gestört noch manipuliert werden können. Erste Ansätze sind auf dem Markt verfügbar. Diese genügen jedoch der kommenden Verbreitung nicht.