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.

Voice over IP ist zu einem ständigen Begleiter geworden.

VON ANDREAS WISLER*

Bis 2008 werden über 90 Prozent aller neuen Telefonzentralen auf Voice over IP basieren. So hat es jüngst Gartner in einer Studie veröffentlicht. Dass dies zu einem Dauerthema geworden ist, zeigen auch die zahlreichen Berichte in verschiedenen Medien. Eine solche Verbreitung zieht Hacker und Cracker magisch an. Grund genug, sich 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 Gefahrenpotentiale für VoIP-Netze, -Endgeräte und –Anwender umfassend beschrieben. Die genannten Gefahren teilen sich in soziale Angriffe, Lauschangriffe, Gesprächskontrolle und Störungen auf.

Soziale Angriffe

Diese Art von Angriffen zielt auf die Persönlichkeit einer Person. Es wird versucht, möglichst viele Informationen über die Person zu sammeln, 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 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.

Mit 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 E-Mails bereits unrühmlich bekannt, nimmt auch Spam über VoIP-Medien 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 E-Mail-Adressen, nur vertrauenswürdigen Personen und Institutionen die eigene Rufnummer bekannt geben.

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, welche diese Arbeit automatisch übernehmen. Jedoch kann nicht einfach ein Kabel *angezapft* werden, sondern die Pakete müssen über den eigenen Rechner umgeleitet werden. Diese Möglichkeit wird *Man in the middle Attacke* genannt. Damit dies erst möglich wird, muss der Benutzer dazu gebracht werden, eine Software einzuspielen. Hier kommt wieder der soziale Faktor als wichtigstes Argument. 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. Ein solches Tool ist zum Beispiel Cain&Abel. Mit einfachsten Mitteln ist es möglich, VoIP-Datenpakete abzufangen und als normale Musikdatei abzuspeichern. So kann das Gespräch auch zu einem späteren Zeitpunkt in Ruhe abgehört werden.

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. Weitere Auswirkungen können sein:

Umleitung von Datenströmen:
- ► Abhören der Sprachdaten (Integrität, Vertraulichkeit)
- ► Auslesen von Registrierungsvorgängen an Voice-over-IP-Servern bzw. Gateways (Integrität, Authentizität, Vertraulichkeit)
- ► Manipulation bzw. Modifikation der übertragenen Daten (Integrität, Authentizität, Vertraulichkeit)
- ► Übernahme von Verbindungen bzw. Sitzungen (Authentizität, Integrität)
- ► Identitätsbetrug (Authentizität, Integrität)
- ► Verhinderung der Kommunikation (Verfügbarkeit)
- ► Gebührenbetrug (Authentizität)

Beeinträchtigung der Dienstgüte:
- ► Verzerrung der Sprachkommunikation (schlechte Sprachverständlichkeit) (Verfügbarkeit)
- ► Verlangsamung von Verbindungsauf- und -abbau (Verfügbarkeit)
- ► Fehlerhafte Gebührenerfassung (Integrität)

► Ausfall einzelner Endgeräte oder Gruppen von Geräten (Verfügbarkeit)

Störungen

Anders als bei der bekannten Telefonie, können Voice over IP Geräte mit relativ kleinem Aufwand gestört werden. Zu den bekanntesten Angriffen zählt DoS (Denial of Service). Ziel ist es, die Infrastruktur so zu *beschäftigen,* dass ein normaler Betrieb nicht mehr möglich ist. Wahlweise 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. Passende Schutzmöglichkeiten umzusetzen, ist jedoch nicht einfach. Nicht alle Hersteller implementieren die Standard-Voice-over-IP Protokolle in der gleichen Art und Weise, obwohl im SIP-Standard bereits verschiedene Sicherheitstechniken vorgesehen oder integriert sind.

So gibt es etwa eine grundlegende Authentifizierung und Autorisierung für Anwender und Proxies per Digest Authentication. Dabei wird mit Hilfe der Kryptografie und einer Einweg-Funktion ein Wert berechnet. Aus diesem Wert kann der Ursprung nicht mehr gebildet werden. Auch Signatur- und Verschlüsselungsmöglichkeiten für die Nachrichten sowie ein Tunneling-Modus für die SIP-Header sind vorgesehen. Dafür wird allerdings eine Public-Key-Infrastructure (PKI) vorausgesetzt. Auch für die eigentliche Kommunikation zwischen den Teilnehmern liegt mit dem Secure Real-time Transport Protocol (SRTP) eine sichere Lösung vor.

Da die Lösungen für eine sichere PKI Umgebung noch in den Kinderschuhen stecken, setzen zahlreiche Hersteller auf das Virtual Private Network (VPN). Eine solche Verbindung ist zwar gegen eine Vielzahl von Angriffen immun und damit sehr sicher, jedoch werden die möglichen Kommunikationspartner stark eingeschränkt. Nur wer auch VPN einsetzt, kann noch erreicht werden.

Um nicht auf Resultate der Hersteller zu warten, hat Phil Zimmermann, der Entwickler von PGP, eine Lösung zur Verschlüsselung von Voice-over-IP Datenpaketen entwickelt: Zfone. Diese Software funktioniert mit den meisten auf dem Markt verfügbaren Geräten und ist sehr einfach in der Anwendung. Somit kann der eigene Telefonverkehr nicht mehr abgehört werden.

Das der Software zugrunde liegende Protokoll ZRTP hat Phil Zimmermann an die Internet Engineering Task Force (IETF) weitergegeben, um es als öffentlichen Standard anerkennen zu lassen. ZRTP nutzt einen Algorithmus für öffentliche Schlüssel, ohne von einer Public-Key-Infrastruktur (PKI) abhängig zu sein. Zudem werden keine gleichbleibenden Schlüssel verwendet. ZRTP soll zudem Man-in-the-Middle-Attacken aufspüren und verhindern können. Am Ende eines Telefonats werden die Schlüssel zerstört, sodass auch abgefangene Schlüssel wertlos werden. Sämtliche Authentifizierungen wickelt Zfone über das Real-Time Transport Protocol (RTP) ab.

Ein effektiver Schutz kann im Moment aber nur bei den Herstellern oder beim Provider geschehen. Sie müssen Dienste und Möglichkeiten integrieren, die weder gestört noch manipuliert werden können. Erste Ansätze sind auf dem Markt verfügbar. Diese genügen jedoch der kommenden Verbreitung (noch) nicht.

** Andreas Wisler ist dipl. Ing. FH, CISSP und Geschäftsführer der GO OUT Production GmbH.*

Die Software funktioniert mit den meisten auf dem Markt verfügbaren Geräten

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 möglich.