von Dr. Ivan Roman*

Die VoIP-Sicherheit im Visier der Hacker

Voice over IP (VoIP) gehört zu den bedeutendsten Entwicklungen der letzten Jahre innerhalb der Informationstechnologie. Bei der ganzen Begeisterung besteht jedoch die Gefahr, dass die Sicherheitsproblematik ausser Acht gelassen wird.

VoIP bietet viele Möglichkeiten und Vorteile. Angefangen bei kostenlosen Gesprächen zwischen Internettelefonie-Nutzern, über günstige Angebote für den Zugang in die klassischen Telefonienetze bis hin zur Integration von Daten- und Sprachkommunikation in Firmen. Die Sprachtechnologie kann die Betriebskosten reduzieren und ermöglicht neue Anwendungen. Doch es gibt auch Schattenseiten. Das Lösen von Sicherheitsfragen hinkt der Verbreitung der neuen Technologie noch hinterher. Dies bildet einen guten Nährboden für Angreifer.

Wo liegen die Gefahren?

Wie der Name bereits sagt, handelt es sich bei VoIP um eine IP-basierende Technologie. Man verlässt die gewohnte, scheinbar völlig gesicherte Plain-Old-Telephone-Service-(Pots-) Umgebung und steigt in die «böse», durch Viren und Hacker gefährdete IP-Welt ein. Daher ist VoIP primär denselben Gefahren ausgesetzt wie die IP-Infrastruktur. Zusätzlich kommen noch einige VoIP-spezifische Gefährdungen hinzu.

Bei der Sicherstellung der IT-Sicherheit geht man in der Regel von drei Grundanforderungen aus. Zunächst stellt sich die Frage, ob der Verkehr vor unberechtigtem Mitlesen und Mithören geschützt ist (Vertraulichkeit), sodann, ob die Daten unverfälscht am Zielort ankommen (Integrität) und schliesslich, ob die Verfügbarkeit des Dienstes gewährleistet

CHECKLISTE: ANFORDERUNGEN AN VOIP-SYSTEME

- VoIP-Protokolle gemäss den eigenen Anforderungen wählen
- Anwender trainieren und sensibilisieren
- Starke Zugangskontroll- und Authentifizierungssysteme installieren
- Daten gegen Lauschangriffe und Verfälschung schützen
- VoIP-Infrastruktur gegen DOS-Angriffe schützen
- Erreichbarkeit der Notfallnummern überprüfen
- Daten- und Sprachverkehr trennen
- Remote-Operationen kontrollieren
- Einsatz von Firewalls und NAT abklären
- Neuentwicklungen im Auge behalten

ist (Verfügbarkeit). Diese Methode lässt sich auch für die Betrachtung der VoIP-Sicherheit anwenden.
Es gibt eine ganze Reihe von Angriffsformen, die eine oder mehrere «Stützen» der VoIP-Sicherheit gefährden können. Zu den wichtigsten Gefährdungen gehören die Lauschangriffe, die Denial-of-Service-(DoS-) Angriffe und Spam over Internet Telephony (Spit). Einige Angriffe sind ziemlich einfach zu bewerkstelligen, andere eher mit viel Aufwand und entsprechend hoher krimineller Energie verbunden.

Lauschangriffe

Die Lauschangriffe gehören zu den klassischen Angriffstypen; sie greifen die Vertraulichkeit der Informationen an. Dies ist an sich nicht Neues, lassen sich doch bekanntlich bereits die klassischen Telefonieanschlüsse abhören. Auch bei den drei im professionellem Umfeld eingesetzten VoIP-Verfahren H.323, SIP, SCCP (vgl. Kasten) ist dieser Angriff sehr gut möglich. Die ITU-Empfehlung H.323, das Cisco Protokoll SCCP sowie das zunehmend häufiger eingesetzte IETF-basierende SIP-Protokoll definieren zwar verschiedene Signalisierungsprotokolle, für den eigentlichen Sprachtransport setzen aber alle das RTP (Real-Time Transport Protocol) ein.
Der RTP-Datenstrom ist standardmässig unverschlüsselt. Mit im Internet frei verfügbaren Werkzeugen wie «Ethereal» oder «Cain & Abel» lassen sich die RTP-Pakete mitschneiden, als Audiodatei abspeichern und später abspielen. Die Voraussetzung dafür ist der physikalische Zugang zum entsprechenden Netzwerk. Hacker können solche Daten an einem Hub mitlesen, oder durch Modifikation so genannter ARP-Tabellen den Verkehr im geswitchten Umfeld entsprechend umleiten.
Wesentlich gefährdeter sind drahtlos geführte VoIP-Gespräche – sofern sie nicht genügend geschützt sind. Als Bedrohungsszenarien sind etwa das Abhören einer PIN-Abfrage oder eines vertraulichen Arztgespräches denkbar. Das so genannte Sniffing eines Signalisationskanals bringt keine Sprachinformationen hervor, jedoch die Angaben, wer mit wem wann kommuniziert hat. Je nach Einsatz führt dies zu einer unerwünschten Verminderung der Vertraulichkeit.

Denial-of-Service-(DoS-)Angriffe

Die Verfügbarkeit des Sprachdienstes ist ein zentraler Aspekt, der erhöhte Aufmerksamkeit verdient. Bekannt ist etwa die Problematik, dass sich Notrufe im VoIP-Netz in vielen Fällen nicht zurückverfolgen lassen, weil sich nicht feststellen lässt, woher der Anruf getätigt wurde. Zudem ist es offensichtlich, dass eine nicht funktionierende Telefoninfrastruktur für Unternehmen enorme wirtschaftliche Einbüssen und auch Imageschäden nach sich ziehen kann.
VoIP-Systeme umfassen Einzelkomponenten wie Server, Switches und IP-Telefone. Dabei handelt es sich um klassische IT-Systeme, die als solche auch den klassischen DoS-Angriffen wie etwa «Buffer Overflow» (Überflutung) ausgesetzt sind.
DoS-Angriffe sind auch auf den Signalisations- oder Datenpfad möglich. So verwendet etwa das SIP-Protokoll verschiedene Befehle («Cancel», «Bye») und Antwort-Codes, die sich für einen DoS-Angriff – zum Beispiel einen Sitzungsabbruch – missbrauchen lassen. Ähnliche Resultate erzielt man mit dem Einfügen von Daten mit hohen RTP-Nummern im Datenpfad.

Spam over Internet Telephony (Spit)

Unter den derzeit aktuellsten Gefährdungen nimmt Spam eine der führenden Positionen ein. Bei VoIP dürfte sich die Situation noch verschärfen. Analog zu SMTP erfolgt bei SIP keine automatische Kontrolle des Ursprungs der Nachricht. Dies ermöglicht den Einsatz von gefälschten Absender-Identitäten und das Senden grosser Mengen unerwünschter Meldungen.
Zusätzlich besteht die Möglichkeit, durch den Missbrauch des so genannten Register-Befehls alle registrierten Geräte aufzulisten (Directory Harvesting). Es ist nicht schwierig, sich ein Szenario vorzustellen, in dem die Voice-Mailbox voll von automatischen Anrufen ist, die «garantiert» echte Rolex-Uhren, billige Software oder Potenzmittel anpreisen. Die Begeisterung darüber dürfte sich in Grenzen halten.

Fazit

VoIP ist eine zukunftsträchtige Technologie und immer mehr Firmen setzen sie ein. Sie ist jedoch mit diversen Sicherheitsgefährdungen behaftet. Die Sicherheitsprobleme lassen sich jedoch bewältigen. Wer VoIP einsetzen möchte, sollte die Sicherheitsaspekte von Anfang an berücksichtigen und nicht erst in einer späteren Phase. So lassen sich teure nachträgliche Modifikationen vermeiden. ■

*) Dr. Ivan Roman ist Geschäftsleiter der Roman-Consulting & Engineering AG, Zürich

VOIP GLOSSAR

H.323: ITU-T-«Rahmenempfehlung» zur Übertragung von Multimediainhalten über paketbasierte Netze
H.235: ITU-T-Sicherheitsempfehlung (Verschlüsselungs- und Authentifizierungsmethoden) für H.323 und andere H.245-basierende Terminals
H.245: ITU-T-Empfehlung für Steuerung logischer Kanäle beim Auf- und Abbau für die Audio- und Video-Übermittlung
RTP (Real-Time Protocol): Transport-Protokoll zur kontinuierlichen Übertragung von audiovisuellen Daten (Streams) über IP-basierte Netzwerke (RFC 3550 …)
RTCP (Real-Time Control Protocol): Kontrollprotokoll für RTP
SRTP (Secure RTP): AES-Verschlüsselung von Echtzeitdaten, (RFC 3711)
SIP (Session Initiation Protocol): Signalisierungs-Kontroll-Protokoll mit dem Multimedia-Sitzungen eingerichtet, unterhalten und beendet werden. (RFC 3261 – 3265 …)
SIPS (SIP Secure, SIP over SSL): Einsatz von SIP über TLS/SSL
SCCP (Skinny Client Control Protocol): Von Cisco entwickeltes Protokoll, das in den VoIP-Produkten von Cisco Verwendung findet