Network Academy Day

VoIP-Security

Skype versus Asterisk

Dr.-Ing. Kai-Oliver Detken
URL: http://www.decoit.de
URL2: http://www.detken.net
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

Portfolio der DECOIT GmbH

- **Solutions (Lösungen)** zur Identifizierung der Probleme und Angebot einer Lösung innerhalb eines Pflichtenhefts für die Umsetzung des Projekts
- Kundenorientierte **Workshops, Coaching, Schulungen** zur Projektvorbereitung und -begleitung
- Nationale und internationale **Förderprojekte** auf Basis neuer Technologien, um neues Know-how aufzubauen oder Fördermöglichkeiten aufzuzeigen
- **Technologie- und Markttrends**, um strategische Entscheidungen für und mit dem Kunden vor einer Projektrealisierung treffen zu können
- **Software-Entwicklung** zur Anpassung von Schnittstellen und Internet-Projekten
- Schaffung innovativer **Produkte**

Consultancy & Internet Technologies

Inhalt

- Stand der Technik
- Open Source Projekt Asterisk
- Skype-Lösung
- Bedrohungen und Attacken
- Angriffstools
- Protokoll-Risiken
- Fazit und Empfehlungen

Voice-over-IP (VoIP)

- Sprachdaten, die über ein IP-basiertes Datennetz transportiert werden
- Dabei sind Echtzeitdaten im Weitverkehrsumfeld gemeint
- VoIP hängt in seiner Qualität stark von den Begebenheiten der Internet-Protokolle ab
- VoIP kann dabei sehr unterschiedlich, stark anhängig vom Hersteller, realisiert werden

IP-Telefonie (IPT)

- IP-Telefonie beschränkt sich auf den lokalen Bereich und meint vornehmlich den Einsatz von IP-Endgeräten zur VoIP-Kommunikation
- Mittels VoIP ist die Anbindung an bestehende TK-Netze möglich
- Endgeräte für IP-Telephonie sind mannigfaltig am Markt vorhanden
- Software-basierte Lösungen sind neben Hardware-Geräten verfügbar (u.a. über die TAPI-Schnittstelle)

VoIP-Szenarien

- Campus VoIP: es wird eine Nebenstellenanlage auf IP-Basis verwendet, die auch als IP-PBX bezeichnet wird. IP-Telefone und/oder Softphones sind mit dieser IP-PBX verbunden. Der Verbindungsaufbau in das öffentliche Telefonnetz wird über Gateways ermöglicht. Diese Variante ist schwer von außen zu attackieren, da die Telefongespräche nicht über das Internet oder andere unsichere Netze geführt werden.
- IP Centrex / Hosted IP: beinhaltet eine virtuelle, IP-basierte PBX, die von einem Provider zur Verfügung gestellt wird. Der Provider ist hierdurch in der Lage, eigene Sprachdienste anzubieten, ohne dass ein Unternehmen eigene Gateways oder PBX-Systeme anschaffen muss. Aus Sicht des Unternehmens muss nur eine ausreichende Internet-Anbindung vorhanden sein und IP-Telefone und/oder Softphones müssen angeschafft werden. Attacken auf das VoIP-System können über das Intranet oder über das Internet (aus dem Providernetz) erfolgen.
- VoIP-Trunks: VoIP-Trunkverbindungen lösen zunehmend herkömmliche verbindungsorientierte Telefonverbindungen ab. Dabei kann es zu einem höheren Angriffspotenzial kommen, wenn die Übertragung über unsichere Netze realisiert wird.

Protokolle und Standards bei VoIP

<table>
<tr><td>Audio-Applikationen</td><td>Video-Applikationen</td><td colspan="4">Terminal Kontrolle und Management</td><td>Daten</td></tr>
<tr><td rowspan="2">G.711
G.722
G.723
G.728
G.729</td><td rowspan="2">H.261
H.263</td><td rowspan="3">RTCP</td><td rowspan="3">Terminal zu Gatekeeper Signalisierung

RAS</td><td rowspan="3">H.255.0
Q.931
Verbindungs-signalisierung (Call Setup)</td><td rowspan="3">H.245 Kontroll-kanal</td><td>T.124</td></tr>
<tr><td rowspan="2">T.125</td></tr>
<tr><td colspan="2">RTP</td></tr>
<tr><td colspan="4">Unzuverlässiger Transport (UDP)</td><td colspan="2">Zuverlässiger Transport (TCP)</td><td rowspan="3">T.123</td></tr>
<tr><td colspan="6">Netzwerkschicht (IP)</td></tr>
<tr><td colspan="6">Sicherheitsschicht (IEEE 802.3)</td></tr>
<tr><td colspan="7">Bitübertragungsschicht (IEEE 802.3)</td></tr>
</table>

Open Source Projekt Asterisk (1)

- Asterisk ist eine Software PBX (Private Branch eXchange) die unter Linux, BSD und OS X läuft
- Dabei ermöglicht Asterisk verschiedene Telefonnetze miteinander zu verbinden.
- Diese Netze können VoIP Netze sein z.B. SIP, IAX, H.323 oder auch ISDN
- Dazu verwendet Asterisk so genannte Channel Treiber die miteinander kommunizieren können
- Durch die Vielzahl von unterstützten Protokollen und Funktionen, eignet sich Asterisk für Gateways zwischen verschiedenen Netzen, als Konferenzserver sowie als Server für Sprachmenüs und automatisierte Steuerung durch den Anrufer
- Mittels CTI können Desktop Applikationen angebunden werden
- Durch Scripting-Möglichkeiten lässt sich Asterisk nahezu beliebig konfigurieren und erweitern

Open Source Projekt Asterisk (2)

- Leistungsmerkmale
  - Standard Call Features: CLI, Transfer, Parking, DnD …
  - Konferenzräume mit >3 Teilnehmern (MeetMe)
  - Wartemusik (MoH)/verschiedene Formate u.a. MP3
  - Mischbetrieb Anlagen- und Mehrgeräteanschluss, S0/S2M
  - Message Waiting Indication (MWI)
  - SMS im Festnetz
  - Anrufwarteschlange: ACD, Call-Queue
  - Gesprächsdatenerfassung
  - Flexible Externgesprächsberechtigungen
  - DISA (Direct Inward System Access)
  - VoiceMail System: Abruf über Telefon mit PW-Schutz, Zustellung per E-Mail, Web-Access
  - Default- und individuelle Ansagen: verschieden für „nicht erreichbar“ oder „besetzt“
  - FaxMail System: Fax Mailbox, Zustellung über E-Mail
  - Sprachdialogsystem (IVR)
  - Telefonbuch zentral und individuell

Open Source Projekt Asterisk (3)

- Unterstützte Protokolle & Codecs
  - Protokolle
    - SIP
    - H.323
    - MGCP
    - SCCP/Skinny
    - IAX/IAX2
  - Codecs:
    - G.723.1
    - G.711 (μ-Law, A-Law),
    - GSM
    - ADPCM
    - G.729
    - iLBC
    - MP3

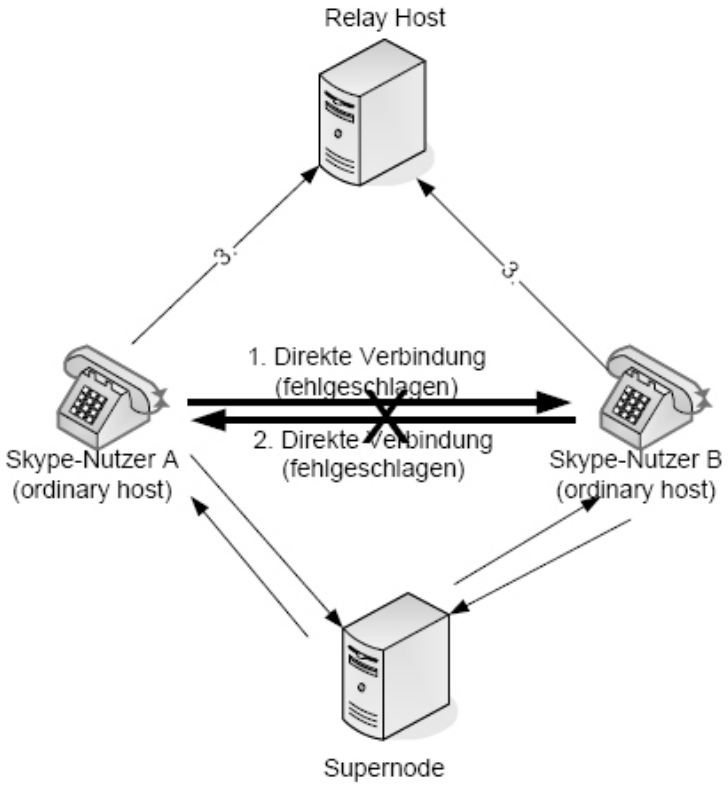
Skype

- Skype ist eine Entwicklung von Niklas Zennström und Janus Friis, die bereits durch die Gründung von KaZaA bekannt sind. Deshalb basiert Skype ursprünglich auf einer Peer-to-Peer-Architektur (P2P)
- Die Internet-Telefonie-Anwendung Skype ermöglicht Telefongespräche zwischen PCs, mobilen Endgeräten sowie zwischen PC und Fest- bzw. Mobilfunknetz
- An Betriebssystemen werden Windows, MacOS, Linux bzw. PocketPC und Windows Mobile unterstützt
- Neben der Telefonie sind Chat, Videokonferenz, File- und SMS-Transfer und über externe Anwendungen und Plug-ins auch z.B. Desktop-Application-Sharing (z.B. festoon, Unyte) möglich
- Dabei ist zum Telefonieren der Einsatz eines PCs inzwischen nicht mehr zwingend erforderlich. Einige Hersteller bieten auch Skype-fähige Telefone (z.B. schnurlos über WLAN) an
- Die Sprachqualität von Skype ist aufgrund der Verwendung neuer Codecs recht hoch (innerhalb des IP-Netzes). Verwendet werden derzeit: SVOPC (16 kHz), AMR-WB (16 kHz), G.729 (8 kHz), G.711

Elemente von Skype (1)

- Skype ist ein „Overlay-Netz“, in dem es hauptsächlich zwei Arten von Knoten gibt:
  - Hosts: versenden von Mediendaten und Textnachrichten
  - Supernodes: besitzen öffentliche IP-Adressen, ausreichende Rechnerressourcen (CPU, RAM), ausreichende Bandbreite
- Die Struktur von Skype ist im Rahmen des P2P-Netzes (FastTrack) teilweise dezentral, beispielsweise das Telefonbuch. Die Authentifizierung und das Abrechnen hingegen erfolgen über einen zentralen Rechner.
- Das Skype-Netz setzt auf vorhandene Netztechniken auf: Skype-Clients müssen eine eigene Tabelle (Host Cache) mit erreichbaren Knoten abbilden und aktualisieren. Der Host Cache enthält IP-Adressen und Ports der Supernodes.
- Durch die P2P-Technologie verbraucht Skype relativ viel Bandbreite: 3-16 kbyte/s wird pro Gespräch verbraucht (Durchschnittlich: 30 Mbyte/Stunde), wodurch im Monat bei einstündigen Gesprächen pro Tag ca. 1 Gbyte bedeuten würde. Dies ist gerade für die Unternehmenskommunikation ein hoher Wert.

Elemente von Skype (2)



- Der Relay Host ähnelt dem Supernode, spielt jedoch im Skype-Netz eine andere Rolle
- Er agiert als „Data-Transfer Relay Station“. Seine Aufgabe besteht darin, Daten für die Clients zu übertragen, die sich nicht direkt mit anderen Peers verbinden können.
- Diese Art des Verbindungsaufbaus wird realisiert, wenn sich beide Kommunikationspartner jeweils hinter restriktiven Firewalls befinden und keine direkte Verbindung miteinander aufbauen können

Skype versus Asterisk

Skype

- Die Software arbeitet hinter den meisten Firewalls und NAT-Routern problemlos, da für die Kommunikation u.a. eine Variante des STUN-Protokolls zur Verbindung verwendet wird
- Das Skype-Protokoll wird mittels AES256 verschlüsselt und mittels RSA übertragen
- Das Protokoll ist proprietär und kann nicht mit anderen VoIP-Lösungen kommunizieren
- Plug-Ins für andere Programme existieren (z.B. Miranda IM) durch eigene API
- SkypeOut Dienst zu anderen Telefondiensten besitzt eine relativ schlechte Qualität
- Herkömmliche IP-Telefone lassen sich nicht einsetzen
- Zur Kommunikation wird ein Skype-Server im Internet benötigt
- Die Software lässt sich in Handys oder PDAs leicht integrieren und mobil nutzen

Asterisk

- Asterisk arbeitet als interne PBX oder als virtuelle Telefonanlage beim Provider
- Es werden VoIP-Standards verwendet (mit Ausnahme des IAX/IXA2-Protokolls)
- Interoperabilität wird mit anderen VoIP-Lösungen durch Standards gewährleistet
- UMS-Funktionalität ist bereits in der Basis enthalten und kann auch im Zusammenspiel mit anderen VoIP-Systemen verwendet werden
- Telefonie zu ISDN-Netzen und über das Internet wird beides in der gleichen Qualität unterstützt
- Es können IP-Telefone und/oder ISDN-Telefone eingesetzt werden
- Durch CAPI-Schnittstelle können beliebige Applikationen mit Asterisk verbunden werden
- Die Kommunikation kann über Standardprotokolle oder IAX2 verschlüsselt werden
- Die Verwaltung von Asterisk ist mit hohem Linux Know-how verbunden

Bedrohungen und Attacken

- Netzwerkattacken
  - Denial-of-Service (DoS)
  - ARP, MAC, IP, UDP, IRDP Spoofing
  - SYN-, PING- oder MAC-Flooding
  - TCP-Session-Hijacking
  - RST-Attack
  - Data Injection through ISN-Guessing
  - Sniffing
  - Replay
- Angriffe gegen die Applikationsschicht
  - Abfangen der Anschlussgebühren
  - Rufmanipulation
  - Nichtautorisierte Nutzung (Phreaking)
  - Dialer
  - Verletzung der Privatsphäre
  - Spam over IP Telephony (SPIT)

Angriffstools

- Cain & Abel: bedient sich dem ARP-Spoofing, d.h. es werden ARP-Abfragen vorgetäuscht und MAC-Adressen gefälscht, wodurch der Sprachverkehr umgeleitet und abgehört werden kann.
- Vomit: wandelt ein Cisco-basiertes IP-Telefongespräch in ein WAV-File um, die mit jedem Audio-Player abgespielt werden kann. Vomit erfordert eine tcpdump-Ausgabedatei. Es arbeitet nur mit dem G.711-Codierungsstandard zusammen.
- VoIPong: erkennt und filtert VoIP-Calls in einem Datenstrom heraus. Es legt eine Kopie eines G.711-Gesprächs an und konvertiert dieses in ein WAV-File. Unterstützt werden die Protokolle SIP, H.323, SCCP, RTP und RCTP.
- SIP Vulnerability Scanner (SiVuS): untersucht VoIP-Installationen auf Fehler. Dies wird durch das Initiieren von Attacken vorgenommen. Es können auch eigene SIP-Nachrichten generiert werden.
- SIPcrack: als Protokoll-Login-Cracker enthält es zwei Programme: SIPdump, um die eingelogten SIP-User zu finden und SIPcrack, um die Passwörter der gefundenen SIP-User mittels Bruteforce-Attacks zu ermitteln.
- RingAll: ermöglicht DoS-Attacken auf ungeschützte SIP-Clients

Protokoll-Risiko: H.323

- Angriffspunkte
  - Wesentliche Angriffspunkte sind Täuschung der Identität seitens des anrufenden Teilnehmers sowie Manipulation der Nachrichten mit Hilfe von MitM-Attacken.
  - Auch können beim Verbindungsaufbau die Transportadressen der Sprachströme verändert werden, wodurch diese an eine beliebige IP-Adresse umgeleitet, und dort abgehört, aufgezeichnet oder gar verändert weitergeleitet werden können. Diese Bedrohungen betreffen Endgeräte ebenso wie Gateways.
- Absicherung
  - Sicherheit und Verschlüsselung für H.323 und H.245 basierte Terminals durch H.235
  - Authentifizierung mittels verschiedener Algorithmen sowie Datenschutz, welcher durch Verschlüsselung, erreicht wird
  - SSL/TLS wird zur Sicherung der H.245- und H.225.0-Kontrollkanäle verwendet
  - Ein H.235-basierter Gatekeeper kann sicherstellen, dass nur vertrauenswürdige Endpunkte Zugang zu den Diensten des Gatekeepers gewährt bekommen

Protokoll-Risiko: SIP

- Angriffspunkte
  - SIP bietet eine Sicherung der Nachrichten unter Verwendung kryptographischer Hashes und Verschlüsselungs-mechanismen. Dies erlaubt eine zuverlässige Authentifizierung und Absicherung gegen Veränderungen der Signalisierungsnachrichten
  - Allerdings sind nicht alle Header durch Hashing abgedeckt, wodurch eine Manipulation der Absenderkennung möglich ist
  - Wird keine Absicherung der SIP-Nachrichten mit Hashes vorgesehen, so können die im Bereich H.323 beschriebenen Angriffe sogar mit noch einfacheren Mitteln realisiert werden, da die Nachrichten im ASCII-Text codiert werden
  - Auch hier sind Endgeräte und Gateways betroffen
- Absicherung
  - SIP wurde um diverse Sicherheits-mechanismen wie TLS, HTTP Digest, IPsec mit IKE und S/MIME erweitert
  - Es wird Ende-zu-Ende-Sicherheit und Hop-by-Hop-Kommunikation angeboten
  - SIP wird bei Asterisk jedoch nur über UDP realisiert. Das schließt die Absicherung über TLS aus, da dies TCP voraussetzt
  - Die fehlenden Sicherheitsmechanismen für SIP sollen über die nächste Generation des SIP-Channels (Version 3) nachgeholt werden (keine Rückwärtskompatibilität!)
  - Zur Hop-by-Hop-Absicherung gehören TLS und IPsec und zur Ende-zu-Ende-Absicherung zählen SIP-Digest-Authentication und S/MIME
  - S/MIME ist im RFC-3261 allerdings nur optional definiert

Protokoll-Risiko: RTP

- Angriffspunkte
  - Mit den RTP-Informationen kann eine Menge von Datenpaketen einer Verbindung in einer korrekten Reihenfolge mit dem passenden Codec decodiert und auf einem Ausgabegerät abgespielt werden, ohne auf die Signalisierung dieser Verbindung zurückgreifen zu müssen
  - Diese einfache Decodierung des Medienstroms versetzt einen Angreifer in die Lage, die Datenpakete eines Sprachstromes abzuhören und zu manipulieren, sobald er auf diese zugreifen kann
  - Dabei ist sogar die Reihenfolge der empfangenen Datenpakete unerheblich
  - Zwar entstehen Lücken bei der Decodierung, wenn bestimmte Datenpakete fehlen, jedoch ist dies nicht mit einem Synchronisationsverlust des Kanals verbunden
- Absicherung
  - SRTP nimmt eine AES-Verschlüsselung der Medienströme vor
  - Um eine Verschlüsselung zu gewährleisten, muss zunächst ein Schlüsselaustausch erfolgen
  - Durch die Verwendung von SHA-1 werden die Gesprächsteilnehmer authentifiziert
  - Der Schlüssel, welcher genutzt wird, um die Nutzdaten zu verschlüsseln, wird allerdings über SIP übertragen
  - Somit kann der Schlüssel ausgespäht werden, wenn SIP nicht ausreichend abgesichert ist

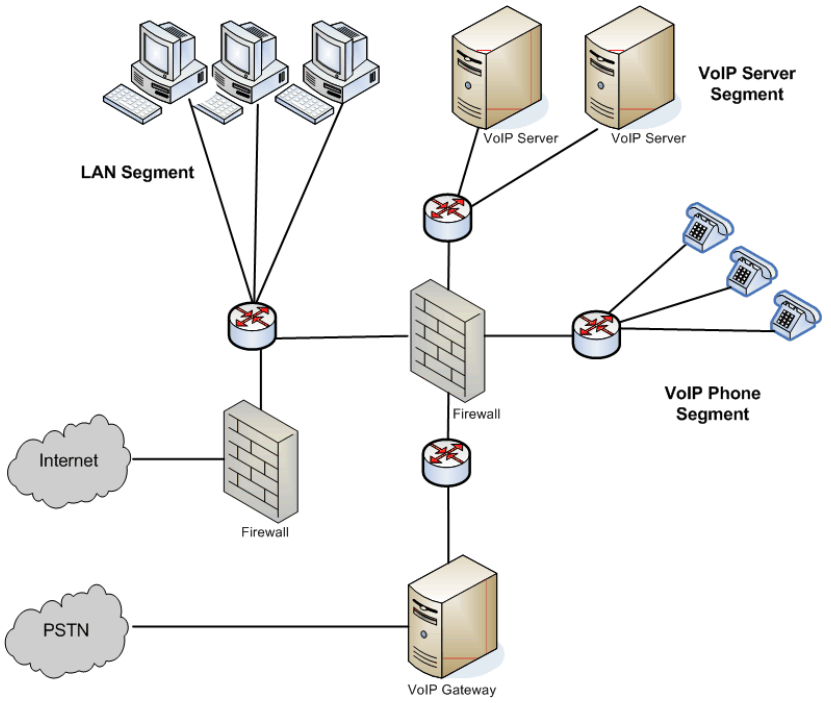
Protokoll-Risiko: IAX/IAX2

- Angriffspunkte
  - Proprietär, jedoch offengelegt
  - Signalisierungs- und Medientransport werden über einen einzigen Port (UDP 4569) abgewickelt. Dadurch ist das Protokoll IAX2 einfach über NAT-Umgebungen zu transportieren und die Regeln in Firewalls sind überschaubar.
  - Im eigentlichen IAX-Protokoll wurden keine Sicherheitsmechanismen verankert. Dies wurde in der Version IAX2 nachgeholt!
  - IAX-Endgeräte sind relativ selten am Markt vorhanden, so dass dieses Protokoll nur in Szenarien mit Asterisk-Servern relevant ist

- Absicherung
  - Es handelt sich bei IAX2 (im Gegensatz zu SIP) nicht um ein textbasiertes, sondern um ein Binärprotokoll
  - Asterisk-Server können sich gegenseitig über eine PKI authentifizieren. Dazu findet ein RSA- oder alternativ ein Diffie-Hellman-Schlüsselaustausch statt
  - Zur Verschlüsselung der Nachrichten wird hier AES mit 128 Bit verwendet
  - Da IAX2 für den Verbindungsaufbau nur einen UDP Port (4569) benötigt, muss auch nur dieser Port in der Firewall geöffnet werden
  - Da die IP-Endgeräte heute bis auf Ausnahmen kein IAX2 unterstützen, muss auf die Sicherheitsmechanismen in der SIP-Spezifikation und SRTP ebenfalls zurückgegriffen werden

Sicherer Einsatz von Asterisk

- IAX2 sollte zwischen Standorten zum Einsatz kommen (optimale Verschlüsselung und Kompression)
- Separation des Daten- und des VoIP-Bereichs über VLANs
- Separate Abtrennung durch Firewalls
- Separate Subnetze für Daten und Sprache
- Einführung von Priorisierung auf den WAN-Strecken (Q-Tag, DiffServ)



Protokoll-Risiko: Skype-Sicherheit

- Identität:
  - Jeder Peer und somit Client muss vor dem Etablieren der Verbindung seine Identität nachweisen. Dabei werden die Privilegien erst mit dem Berechtigungsnachweis über die User-Credentials (Benutzername und Passwort) bestätigt. Der Nutzername muss selbstverständlich einzigartig und eindeutig sein.
- Vertraulichkeit und Verschlüsselung:
  - Sowohl Schlüsselaustausch als auch die Mediendaten (Sprachpakete) werden Ende-zu-Ende verschlüsselt.
- Privatsphäre:
  - Für die Aufrechterhaltung der Privatsphäre sorgt eine Verschlüsselung auf Basis von AES (Schlüssellänge 256 Bits). Die Übertragung der symmetrischen AES-Schlüssel erfolgt asymmetrisch per RSA (Schlüssellänge bis 2048 Bits).

Skype-Sicherheitskritiken

- Da das Skype Protokoll nicht offengelegt ist, kann die Sicherheit nicht von Benutzern oder Unternehmen nachgeprüft werden
- Skype wird in vielen Unternehmensnetzwerken nicht zugelassen, da die eingesetzte Peer-to-Peer-Technologie von den Verantwortlichen als sicherheitstechnisch fragwürdig eingestuft wird
- Durch die Nutzung des Ports 80 und 443 zum Verbindungsaufbau werden die meisten Firewalls hintergangen
- Zentrale Server stehen zudem nicht unter der Kontrolle der jeweiligen Unternehmen und könnten demnach für Angriffe genutzt werden
- Es sind inzwischen einige Sicherheitslücken veröffentlicht worden (u.a. Auslesen von BIOS-Infos durch ausführbare Datei)
- Abhörmaßnahmen werden von Skype selbst ebenfalls nicht komplett ausgeschlossen

Fazit und Empfehlungen

- Das SIP-Protokoll kann nicht in allen in der Praxis anzutreffenden Formen als hinreichend sicher betrachtet werden
- Trotz der Sicherheitsmechanismen von VoIP-Protokollen (z.B. SIP mit Call-IDs auf der Basis von Hashes) bieten sich Angriffsmöglichkeiten für DoS-Attacken
- Das Phreaking könnte mit VoIP ein Revival erleben
- Es besteht gegen VoIP-Systeme i.a. die Möglichkeit „VoIP-Spam“, auch SPIT (Spam over Internet Telephony) genannt, einzusetzen
- Für sicheres VoIP sollte daher aus Unternehmenssicht ein Campus-Szenario betrieben werden, aus dem heraus über ISDN kommuniziert wird
- Zukünftig kann dann eine Anbindung an öffentliche VoIP-Provider vorgenommen werden, wenn die Signalisierungsstandards ein hohes Sicherheitsniveau übergreifend erreicht haben sowie Authentifizierung und Verschlüsselung auch von Providern angeboten werden
- Die Sicherheitserweiterungen der VoIP-Protokolle bieten bei sachgemäßer Nutzung einen hohen Grad an Abhörsicherheit
- Asterisk benötigt zukünftig ein verbessertes Management; wird aber in vielen Herstellerlösungen bereits angwendet
- Skype bleibt eine Insellösung, die hauptsächlich auf den Privatbereich ausgerichtet ist (Ausnahme: Unterstützung mobiler Endgeräte)

Danke für Ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09

Consultancy & Internet Technologies