Entwicklung eines Maßnahmenkataloges und zugehörigem Prüfschema für die Absicherung von Voice over IP Installationen

Diplomarbeit

zur Erlangung des akademischen Grades
Diplom-Informatiker (FH)

an der Fachhochschule Brandenburg
Fachbereich Informatik und Medien

eingereicht am 4. Dezember 2006
von

Paul Lange
geboren am 29.01.1982

Erstbetreuer
Prof. Dr. phil. Barbara Wiesner
Fachhochschule Brandenburg
Magdeburger Str. 50
14770 Brandenburg an der Havel

Zweitbetreuer
Dipl.-Ing. Enno Ewers
HiSolutions AG
Bouchéstraße 12
12435 Berlin

Inhaltsverzeichnis

1 Einleitung

1.1 Ziel der Arbeit

Derzeit ist es gerade im Heimbereich aufgrund von zahlreichen kostengünstigen Angeboten sehr beliebt, über das Internet zu telefonieren. Einzug hat die IP-Telefonie ebenfalls in Unternehmensnetzwerken erhalten. Dies belegt eine Pressemitteilung des Branchenverbandes „BITKOM“, die sich auf Studien von „FGW Online“ und „E-Business-Watch“ beruft [BIT06]. Danach nutzen bereits 11 Prozent der Privathaushalte und 9 Prozent der Unternehmen Internet-Telefonie. Für Unternehmen wird zudem eine Kostenersparnis von bis zu 30 Prozent prognostiziert.

In Unternehmensnetzwerken ermöglicht die IP-Telefonie neben der Kostenersparnis durch konvergierende Netzwerke auch den Aufbau flexibler Netzstrukturen. Diese Netzstrukturen erleichtern die Integration, wie beispielsweise bei der Kopplung von Standorten und erhöhen die Mobilität, welche bei der Anbindung von Heimarbeitsplätzen notwendig ist. Ferner ergibt sich durch die Konvergenz von Anwendungen ein Mehrwert, der mit *Unified-Messaging-* oder *Call-Center-Lösungen* genutzt werden kann. Im Vergleich zur Festnetz-Telefonie existieren inzwischen auch vergleichbare Qualitätsstandards, die zu einer höheren Akzeptanz und einem vermehrten Einsatz von Voice over IP (VoIP) beitragen.

Häufig werden bei der Einführung von VoIP sicherheitsrelevante Aspekte dieser Technologie nicht berücksichtigt. Deshalb wird aktuell vermehrt Aufklärung im Bereich VoIP-Sicherheit betrieben. So existieren bereits einige Arbeiten von Institutionen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI)[1], dem National Institute of Standards and Technology (NIST)[2] und der Voice over IP Security Alliance (VOIPSA)[3], die sich dieser Problematik annehmen und erste Lösungsansätze aufzeigen. Häufig scheitert jedoch eine Beurteilung der sicherheitsrelevanten Aspekte der eigenen VoIP-Infrastruktur an der Frage, wie sich Sicherheitsdefizite erkennen lassen und Sicherheitsmaßnahmen erfolgreich umgesetzt werden können.

Um diesen Prozess des Audits einer VoIP-Infrastruktur zu vereinfachen, soll im Rahmen dieser Diplomarbeit in Zusammenarbeit mit der Firma „HiSolutions AG“ ein Prüfschema entwickelt werden, anhand dessen VoIP-Sicherheitsaudits erfolgreich durchgeführt werden. Die Grundlage für das Prüfschema bildet der in dieser Arbeit ausgearbeitete Maßnahmenkatalog, gegen den die bestehende VoIP-Infrastruktur geprüft wird. Die Prüfung beinhaltet einen Soll-Ist-Vergleich von

[1] [AAG+05]
[2] [KWF05]
[3] [EGJ+05]

Maßnahmen, der mögliche Mängel aufzeigt und folglich eine Beurteilung der Sicherheit ermöglicht.

Die Motivation für die Entwicklung eines Prüfschemas ist, die technische Sicherheit einer VoIP-Infrastruktur anhand einer fest definierten Methodik zu analysieren. Bei auftretenden Schwachstellen und Risiken werden individuell bewährte Methoden und Mechanismen zur Absicherung aufgezeigt. So sollen durch das einheitliche Prüfschema mögliche Fehlerquellen bei der Durchführung von Audits ausgeschlossen und der Auditprozess einer VoIP-Infrastruktur wesentlich vereinfacht werden. Ferner soll das erarbeitete Prüfschema Auditoren und Unternehmen die Möglichkeit geben, eine bestehende VoIP-Infrastruktur anhand von Prüfkriterien auf Sicherheit zu überprüfen und *Best-Practice-Verfahren* zur Beseitigung ausgemachter Gefährdungen bereitstellen.

Da bereits zahlreiche Risiken von VoIP dokumentiert sind[4], soll es in dieser Arbeit weniger um das Aufzeigen neuer Sicherheitsrisiken gehen. Vielmehr wird eine Methodik ausgearbeitet, die helfen soll, Risiken in einer VoIP-Infrastruktur auszumachen und mögliche Gegenmaßnahmen zu bestimmen. Dieser Ansatz ist insofern wichtig, da bisher nur wenige herstellerunabhängige *Best-Practice-Verfahren* im Bereich VoIP verfügbar sind und nur eine geringe Anzahl von Lösungsansätzen für die umfassende Absicherung einer VoIP-Infrastruktur bereitgestellt werden.

[4] [AAG+05; KWF05; EGJ+05]

1.2 Abgrenzung

1.2.1 BSI-Studie VoIPSEC

Die Studie VoIPSEC [AAG+05] ist ein Dokument des BSI und behandelt das Thema VoIP-Sicherheit. Sie bietet für dieses Thema einen umfassenden Überblick über die technischen Grundlagen, die Bedrohungspotenziale und geeignete Sicherheitsmaßnahmen. Zusätzlich werden anhand von Szenarien die Möglichkeiten und Risiken der IP-Telefonie aufgezeigt.

Die vorliegende Arbeit soll bestehende Lösungsansätze aufgreifen und zusätzlich der zunehmenden Nachfrage nach einer Bewertung der Sicherheit von VoIP-Infrastrukturen gerecht werden. Im Gegensatz zur Studie VoIPSEC verfolgt diese Arbeit das Ziel, ein Prüfschema zu entwickeln, anhand dessen VoIP-Audits erfolgreich nach einer vorgegebenen Methodik durchgeführt werden können. Hierbei wird im Gegensatz zum informellen Charakter der VoIPSEC-Studie ein Ansatz gewählt, der wesentlich praxisnäher ist.

Gemeinsam ist beiden Arbeiten die Absicht, Risiken im Bereich VoIP-Sicherheit und Maßnahmen zur Absicherung von VoIP-Infrastrukturen aufzuzeigen. In dieser Arbeit werden Maßnahmen in einem Maßnahmenkatalog zusammengefasst, der darauf ausgelegt ist, individuell für jede VoIP-Komponente ein Maßnahmenset, abhängig vom Schutzbedarf zur Absicherung bereitzustellen (siehe Kapitel 3.2 Module). So geht es weniger darum, Szenarien und mögliche Maßnahmen aufzuzeigen, sondern anhand von gegebenen Prüfkriterien, eine bestehende VoIP-Infrastruktur auf Sicherheitsdefizite zu untersuchen. Angelehnt an die IT-Grundschutz-Vorgehensweise [BSI05a], ergeben sich die durchzuführenden Prüfkriterien, durch die Modellierung und Schutzbedarfsfeststellung der VoIP-Infrastruktur (siehe Kapitel 3.1 Methodik).

1.2.2 IT-Grundschutz

Im folgenden Abschnitt soll der in dieser Arbeit entwickelte Maßnahmenkatalog und das Prüfschema zur Absicherung von VoIP-Installationen gegenüber den IT-Grundschutz-Katalogen [BSI05b] abgegrenzt werden.

Ziel der IT-Grundschutz-Kataloge ist es ein Sicherheitsniveau zu ermöglichen, das dem normalen Schutzbedarf entspricht und Grundlage für hochschutzbedürftige IT-Systeme ist [BSI05b, S. 14]. In dieser Arbeit werden hingegen Sicherheitsmaßnahmen definiert, die für VoIP-Installationen mit dem Schutzbedarf normal und hoch umzusetzen sind.

Grundlage des Prüfschemas ist ein Maßnahmenkatalog, ähnlich dem der IT-Grundschutz-Kataloge, der aufzeigen soll, wie einzelne Maßnahmen innerhalb der VoIP-Infrastruktur umzusetzen sind. Die in dieser Arbeit angewendete Methodik greift dabei das bewährte Baukastenprinzip der IT-Grundschutz-Kataloge auf und ermöglicht so die Modellierung der VoIP-Infrastruktur. Dadurch wird sichergestellt, dass sämtliche Maßnahmen zur Absicherung eindeutig bestimmt werden können.

Die Bausteine der IT-Grundschutz-Kataloge sollen typische Bereiche eines IT-Systems widerspiegeln und somit neben technischen auch organisatorische, personelle und infrastrukturelle Maßnahmen abdecken [BSI05b, S. 14]. Die vorliegende Arbeit konzentriert sich jedoch auf die technische und organisatorische Sicherheit von VoIP-Installationen, die bisher durch die IT-Grundschutz-Kataloge nicht ausreichend berücksichtigt wird. Diese Fokussierung führt dazu, dass im Bereich der Sicherheitsmaßnahmen nicht alle Phasen des Lebenszyklus einer IT-Komponente[5] abgedeckt sind und vorwiegend Maßnahmen für die Planung und Konzeption, den sicheren Betrieb sowie die Absicherung von VoIP-spezifischen Gefährdungen Bestandteil des Maßnahmenkataloges sind.

Zur Ermittlung der Sicherheitsdefizite in VoIP-Installationen wird auf die etablierte Verfahrensweise des Soll-Ist-Vergleichs der IT-Grundschutz-Kataloge zurückgegriffen. Dieser Soll-Ist-Vergleich von Maßnahmenempfehlungen und realisierten Maßnahmen soll jedoch zusätzlich durch die ausgearbeiteten Prüfkriterien wesentlich vereinfacht und praxisnäher ausgelegt werden.

[5] Die Phasen des Lebenszyklus sind nach IT-Grundschutz die Planung und Konzeption, Beschaffung, Umsetzung, Betrieb, Aussonderung und die Notfallvorsorge [BSI05b, S. 10].

2 Grundlagen

2.1 IP-Telefonie

Die IP-Telefonie ermöglicht die Echtzeitübertragung von Gesprächen über IP-basierte Netze. Somit kann für die Übertragung der Sprache und Daten ein gemeinsames Netzwerk genutzt werden und eine bisher notwendige Telefoninfrastruktur entfällt. Die IP-Telefonie wird damit dem Bedarf gerecht, Informationen aus dem Sprach- und Datennetz zu verknüpfen, wie dies bereits durch die Anwendung von Computer Telephony Integration (CTI) angestrebt wurde. Jedoch erfordert die Konvergenz der Sprach- und Datennetze eine hohe Verfügbarkeit des zentralen Netzwerkes.

Die Übertragung der digitalisierten Sprache erfolgt paketweise, wobei die Pakete durchaus unterschiedliche Wege zum Ziel haben können. Dagegen wird im herkömmlichen Fernsprechnetz die Kommunikationsverbindung exklusiv für die Dauer eines Gespräches reserviert. Zu jedem Zeitpunkt steht hierbei ein kontinuierlicher Datenstrom mit fester Bandbreite zur Verfügung. Begrenzender Faktor ist bei der Festnetztelefonie die Anzahl der zur Verfügung stehenden Leitungen. Diese Einschränkung existiert bei der IP-Telefonie aufgrund der paketbasierten Übertragung nicht, da die nicht verwendete Bandbreite durch andere Kommunikationsteilnehmer genutzt werden kann. Vielmehr hängt die Anzahl der gleichzeitigen Verbindungen von Faktoren wie der zur Verfügung stehenden Bandbreite und der Kapazität der IP-Telefonanlage ab.

Werden allerdings Datenströme verschiedener Anwendungen über eine Leitung übertragen, kann eine Anwendung die verfügbare Bandbreite mit der Übertragung großer Datenmengen an sich binden. Dadurch kann bei dem Transport von Sprachdaten mit Echtzeitanforderungen, die Qualität der Sprachübertragung beeinträchtigt werden. Um den Anforderungen einer Echtzeitanwendung gerecht zu werden, kann zum einen die Sprache gegenüber den Daten priorisiert und somit bevorzugt im Netzwerk behandelt werden. Andererseits besteht die Möglichkeit, dass die Bandbreite einer Leitung ausreichend überdimensioniert wird. Diese beiden Ansätze ermöglichen, die Dienstgüte der Sprachübertragung (QoS[6]) sicherzustellen und so die Übermittlungszeit der IP-Pakete (*Delay*), mögliche Schwankungen (*Jitter*) sowie Paketverluste zu minimieren.

Durch die Verwendung des Internetprotokolls besitzt die IP-Telefonie auch die gleichen IP-spezifischen Gefährdungen. Diese resultieren vor allen Dingen daraus, dass sich durch die Nutzung des Internetprotokolls die Intelligenz des Netzwerks zum Endgerät verlagert und diese die Steuerung der Gespräche übernehmen. Somit ergeben sich auch die meisten Gefährdungen aus Angriffen auf Schwachstellen der Endgeräte und zusätzliche Dienste wie QoS werden erst nachhaltig vom

[6]Quality of Service (QoS)

Netzwerk angeboten. Daher sollte beim Einsatz durch die IP-Telefonie, neben dem großen Potenzial, auch der Mehraufwand einer angemessenen Integration und zusätzliche Risikofaktoren berücksichtigt werden.

Bei der Übertragung von Gesprächen wird zwischen der Signalisierung und der Übertragung der Sprachdaten unterschieden. Die Signalisierung realisiert den Auf- und Abbau einer Sprachverbindung und der Modifikation sowie die Verhandlung der Parameter für die Übertragung der Sprachdaten. Die Signalisierungsdaten können wahlweise über das Transmission Control Protocol (TCP) oder User Datagram Protocol (UDP) übertragen werden. Der Austausch der Sprachdaten erfolgt ausschließlich über das verbindungslose UDP. Folglich müssen die Verluste und die Reihenfolge der Sprachpakete durch das Protokoll zur Übertragung der Sprachdaten erkannt beziehungsweise sichergestellt werden. Protokolle, welche die hier beschriebenen Funktionalitäten sicherstellen, werden im folgenden Kapitel 2.2 beschrieben.

2.2 Protokolle

2.2.1 SIP

Das Session Initiation Protocol (SIP) ermöglicht die Signalisierung und Vermittlung von Multimediaverbindungen. Im Kontext von VoIP ermöglicht das SIP die Kommunikation zwischen zwei oder mehreren Teilnehmern und realisiert den Aufbau, die Veränderung und den Abbau der Kommunikationsverbindungen. Für die Übertragung der Echtzeitdaten und Ermittlung der Dienstgüte kommt das Real-Time Transport Protocol (RTP) zum Einsatz, dessen Funktionalität und Aufbau in Kapitel 2.2.4 beschrieben wird [RSC+02].

Im Jahre 1999 wurde das SIP erstmals durch das RFC 2543[7] von der Internet Engineering Task Force (IETF) standardisiert. Eine gegenüber dieser ersten Spezifikation erweiterte und im Bezug zur Sicherheit verbesserte Version liegt heute in Form des RFC 3261[8] vor. Zu den vom SIP bereitgestellten Sicherheitsmechanismen gehört der Schutz vor DoS-Angriffen[9], die Authentifizierung von Nutzer-zu-Nutzer- und Nutzer-zu-Proxy-Verbindungen, der Schutz der Integrität sowie die Verschlüsselung und der Schutz der Privatsphäre. Zusätzlich zur Signalisierung und Vermittlung von Sprachverbindungen ermöglicht SIP eine Ermittlung der Verfügbarkeit sowie die Ortsbestimmung eines Nutzers [RSC+02, Kap. 2, Abstract].

Die Adressierung der Kommunikationspartner erfolgt über eine SIP-spezifische URI[10] *(SIP-URI)*. Der Aufbau einer SIP-URI ist dem einer E-Mail-Adresse sehr ähnlich. Anhand der folgenden SIP-URI soll der Aufbau beispielhaft erläutert werden.

```
sip:benutzer@hostname
```

Dabei steht der erste Bezeichner für das eingesetzte Schema. Dies kann zum einen *sip* oder dessen sichere Variante *sips* sein. Es folgt die Angabe von Benutzer- und Hostname, unter dem ein Nutzer zu erreichen ist [RSC+02, Kap. 4].

Nach [TW05, S. 126 ff.] wird zwischen einer temporären, umgebungsabhängigen SIP-URI (sip:bob@192.168.2.166) und einer von einem Anbieter zugewiesenen, ständigen (sip:bob@anbieter.de) SIP-URI unterschieden. Um über seine ständige SIP-URI erreichbar zu sein, muss sich jeder Nutzer zuvor gegenüber einem *Registrar* mit der ihm zugeordneten umgebungsabhängigen SIP-URI anmelden. Der Zusammenhang zwischen umgebungsabhängiger und ständiger SIP-URI wird in einem *Location-Server* verwaltet, so dass der *Proxy-Server* nach dessen Abfrage zwischen den SIP-URIs vermitteln kann. Der *Location-* und *Registrar-Dienst* ist

[7] [HSSR99]
[8] [RSC+02]
[9] Denial of Service (DoS)
[10] Uniform Resource Identifier (URI)

in der Regel im SIP-Proxy integriert und somit lediglich logisch, jedoch nicht physisch getrennt [TW05; RSC+02].

Das SIP ist ein textbasiertes Protokoll, dass den UTF-8 Zeichensatz zur Codierung der Nachrichten verwendet. Der Austausch von SIP-Nachrichten erfolgt nach dem Anfrage-Antwort-Modell (*Request/Response Model*). Hierbei wird der Sender einer Anfrage (*Request*) in der SIP-Terminologie als User Agent Client (UAC) und der Sender einer Antwort (*Response*) als User Agent Server (UAS) bezeichnet [RSC+02].

Jede SIP-Nachricht beginnt mit einer Startlinie, in der eine Anfrage beziehungsweise eine Antwort eines User Agents (UA) enthalten ist[11]. Darauf folgt ein *Header* mit einem oder mehreren *Header-Feldern*. Mögliche *Header-Felder* und deren Beschreibung sind in der Tabelle 1 zusammengefasst und variieren abhängig vom Nachrichtentyp. Neben einigen zusätzlichen SIP-spezifischen *Header-Feldern*, wie beispielsweise *CSeq* und *CallID*, sind die Übrigen identisch mit denen des Hypertext Transfer Protocols (HTTP) (*From*, *To*). Auf den *Header* folgt ebenfalls abhängig vom Nachrichtentyp ein optionaler *Body*, dessen Inhalt im Header-Feld *Content-Type* spezifiziert ist. Dieser *Body* einer SIP-Nachricht enthält eine Beschreibung des Medienstroms. SIP verwendet zur Vereinbarung der Parameter des Medienstroms das Session Description Protocol (SDP) in einem *Offer/Answer-Modell* nach RFC 3264[12] [RSC+02].

Header-Felder	Beschreibung	zwingend
Via	Transportinformation für den Antwortenden	ja
Max-Forwards	maximale Anzahl von Hops zum Ziel	nein
To	Empfänger der Anfrage	ja
From	Absender der Anfrage	ja
Call-ID	ermgl. Zuordnung zw. UA und SIP-Dialog	ja
CSeq	SIP-Methode der Transaktion	ja
Contact	direkte Kontaktadresse (URI) des UA	nein
Content-Type	Datentyp des Body (z.B SDP oder MIME)	nein
Content-Length	Länge des Body in Bytes	nein

Tabelle 1: SIP-Header-Felder [TW05; RSC+02]

[11] Einige Beispiele für mögliche Anfragen beziehungsweise Antworten gehen aus der im folgenden Abschnitt beschriebenen Beispielkommunikation hervor.

[12] [RS02b]

Neben dem Kommunikationsablauf nach RFC 3261 [RSC+02, Kap. 4, 24.2] zwischen UAC und UAS, soll anhand der Abbildung 1 zusätzlich die Aushandlung der zum Aufbau des Medienstroms benötigten Parameter vereinfacht[13] aufgezeigt werden.

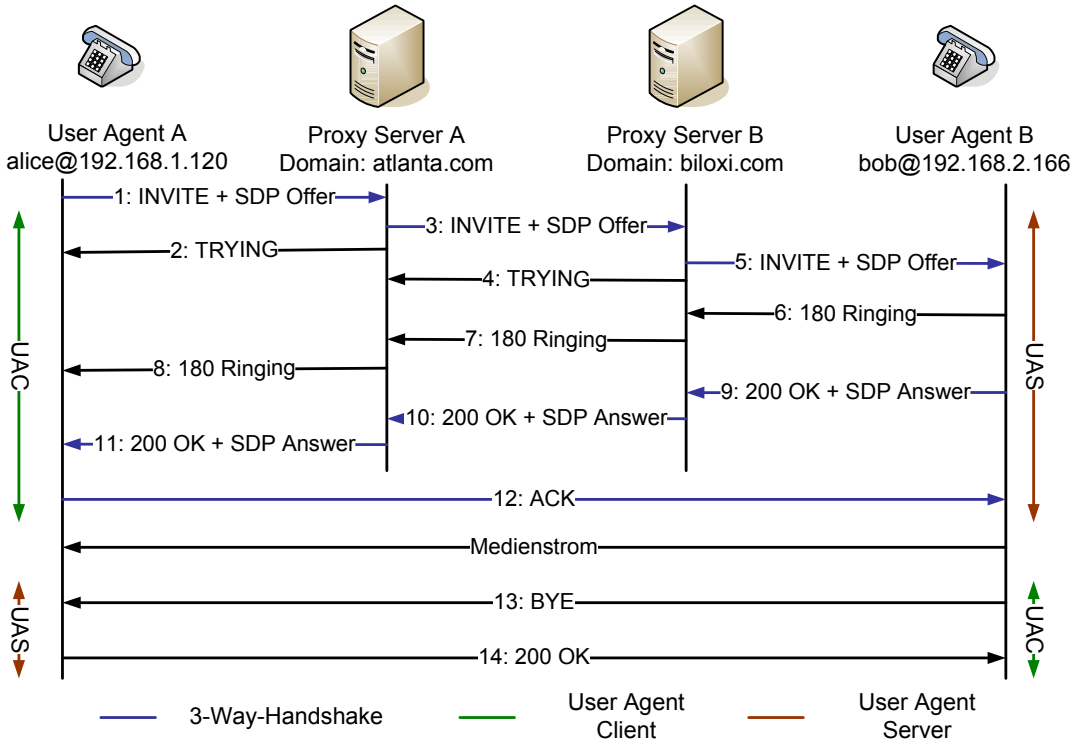

Abbildung 1: SIP-Kommunikation [RSC+02]

1. `INVITE sip:bob@biloxi.com SIP/2.0`

   Die erste Anfrage vom *User Agent A* (Alice) beinhaltet die *INVITE-Methode* mit der ständigen SIP-URI vom *User Agent B* (Bob) und der SIP-Protokollversion. Somit ermöglicht diese Methode gezielt einen Gesprächspartner zum Gesprächsaufbau einzuladen. Alice nimmt innerhalb dieser Anfrage die Rolle des UAC ein. Zusätzlich kapselt die SIP-Nachricht eine SDP-Nachricht *(SDP-Offer)*, welche die zum Aufbau des RTP-Stroms notwendigen Parameter enthält. Dazu gehören unter anderem der übertragene Medientyp, das verwendete Transportprotokoll, der Empfangsport und die IP-Adresse der Sprachverbindung sowie die für die Codierung der Sprachdaten unterstützen Codecs. Bei dieser ersten SIP-Nachricht handelt

[13] Vereinfacht bedeutet in diesem Zusammenhang, dass eine vorherige Registrierung des UA vorausgesetzt wird und die dargestellten SIP-Nachrichten auf die jeweilige Startlinie begrenzt sind.

es sich um die Initialisierung des *3-Wege-Handshakes* zum Aufbau einer SIP-Verbindung. Dieser Mechanismus ist notwendig, da beim Einsatz des verbindungslosen UDP keine Bestätigung der gesendeten Nachrichten erfolgt und somit die erfolgreiche Übertragung innerhalb des SIP sichergestellt werden muss.

2. `SIP/2.0 100 Trying`

   Die auf die Anfrage folgende SIP-Nachricht mit der Statusmeldung *100 Trying* signalisiert Alice, dass die Nachricht vom Proxy-Server A empfangen wurde und die Nachricht zum Ziel weitergeleitet wird.

3. `INVITE sip:bob@biloxi.com SIP/2.0`

   Zunächst muss der Proxy-Server A über eine DNS-Anfrage die IP-Adresse des zur Domain biloxi.com gehörenden Proxys ermitteln. Bevor er die *INVITE-Nachricht* an den Proxy-Server B in der Rolle des UAC weiterleitet, fügt er das in Tabelle 1 beschriebe *Via-Feld* mit seiner SIP-URI hinzu.

4. `SIP/2.0 100 Trying`

   Wenn der Proxy-Server B die *INVITE-Nachricht* erhalten hat, signalisiert er dem Proxy-Server A die Weiterverarbeitung der Nachricht durch die Statusmeldung *100 Trying*.

5. `INVITE sip:bob@192.168.2.166 SIP/2.0`

   Bevor die Nachricht an Bob (UAS) weitergeleitet werden kann, muss der Proxy-Server B die temporäre SIP-URI von Bob über den *Location-Server* erfragen. Nachdem er die Adresse erhalten hat, fügt er das *Via-Feld* mit seiner SIP-URI zum *SIP-Header* hinzu und leitet die Anfrage (*INVITE*) an Bob weiter.

6. `SIP/2.0 180 Ringing`

   Nachdem Bob die Nachricht erhalten hat, klingelt das Telefon und der Anruf kann angenommen werden. Nach dem Erhalt der *INVITE-Nachricht* wird der Zustand des Telefons über die Statusmeldung *180 Ringing* an den Proxy-Server B weitergeleitet.

7. `SIP/2.0 180 Ringing`

   Der Proxy-Server B nutzt die *Via-Einträge* im *Header* des SIP-Paketes, um die Adresse für die Statusmeldung *180 Ringing* zu ermitteln. Anschließend entfernt er den eigenen *Via-Eintrag* im *SIP-Header*. Zusätzliche Anfragen an den *Location-Server* entfallen aufgrund der in den *Via-Feldern* definierten Route.

8. `SIP/2.0 180 Ringing`

   Der Proxy-Server A verhält sich ähnlich seinem Vorgänger und leitet die Nachricht an Alice weiter. Somit erhält Alice die Statusmeldung *180 Ringing* und der ausgehende Rufaufbau kann am Display angezeigt und durch einen Freiton akustisch signalisiert werden.

9. `SIP/2.0 200 OK`

   Wenn der Empfänger des Anrufes (UAS) den Hörer abnimmt, wird dies mit der Statusmeldung *200 OK* dem zugehörigen Proxy-Server B signalisiert. Zusätzlich kapselt die SIP-Nachricht wie bei der ersten INVITE-Nachricht *(1)* eine SDP-Nachricht. In dieser Nachricht *(SDP-Answer)* teilt Bob Alice unter anderem die von ihm aus der *SDP-Offer* unterstützten Codecs sowie seinen Empfangsport und IP-Adresse mit.

10. `SIP/2.0 200 OK`

    Der Proxy-Server B leitet die Statusmeldung an den Proxy-Server A weiter.

11. `SIP/2.0 200 OK`

    Wenn Alice die Statusmeldung *200 OK* empfängt, hört das Klingeln des Telefons auf und signalisiert somit eine aufgebaute Verbindung zwischen den Kommunikationspartnern.

12. `ACK sip:bob@bob@192.168.2.166 SIP/2.0`

    Abschließend wird der Rufaufbau gegenüber Bob durch eine *ACK-Nachricht* direkt bestätigt und somit der *3-Way-Handshake* abgeschlossen. Die direkte Bestätigung ist durch die Verwendung des in Tabelle 1 beschriebenen *Contact-Feldes* möglich. Der Empfang der Nachricht signalisiert Bob, dass Alice nach wie vor den Gesprächsaufbau wünscht. Im Anschluss an den Gesprächsaufbau erfolgt die Übertragung des Telefongespräches gemäß der durch das *Offer/Answer-Modell* des SDP ausgehandelten Parametern. Eine Übertragung der Sprachverbindung durch das RTP wird im Kapitel 2.2.4 RTP & RTCP näher beschrieben.

13. `BYE sip:alice@atlanta.com SIP/2.0`

    Wenn das Gespräch durch das Auflegen des Hörers von Bob beendet wird, initiiert er in der Rolle des UAC direkt eine *BYE-Anfrage* an Alice (UAS). Durch den Wechsel der Rollen zwischen Alice und Bob erhält Bobs Anfrage auch eine neue *Call-ID* (siehe Tabelle 1).

14. `SIP/2.0 200 OK`

    Abschließend bestätigt Alice den Erhalt der *BYE-Anfrage* und somit den Rufabbau durch die Statusmeldung *200 OK*.

Im Folgenden soll die Authentifizierung und Registrierung eines SIP-Teilnehmers (UAC) gegenüber einem *Registrar* beziehungsweise Proxy erläutert werden [TW05; RSC+02]. Zur verschlüsselten Übertragung der Authentifizierungsdaten und zum Schutz vor *Reply-Angriffen* baut der SIP-Standard auf das *HTTP-Digest-Verfahren*[14] auf, im Folgenden *SIP-Digest* genannt. Die Authentifizierung mittels *SIP-Digest* ist vom SIP-Standard zwingend vorgeschrieben. Eine Verwendung der *Basic-Authentifizierung* wird vom SIP-Standard abgelehnt und muss von SIP-Servern nicht mehr beantwortet werden.

Bei der Authentifizierung mittels *SIP-Digest* wird im Gegensatz zur *Basic-Authentifizierung* das Passwort zu keinem Zeitpunkt im Klartext zwischen den Kommunikationsteilnehmern übertragen. Dazu wird eine eingehende SIP-Nachricht mit der Methode *INVITE* oder *REGISTER* eines UAC vom Registrar mit einer der folgenden Statusmeldungen abgelehnt.

`SIP/2.0 401 Unauthorized` (bei einem SIP-Registrar)

oder

`SIP/2.0 407 Proxy Authentication Required` (bei einem SIP-Proxy)

Diese Statusmeldungen enthalten zusätzlich einen sogenannten *Nonce* (Zufallswert), ein *Digest Realm* und den zur Chiffrierung zu verwendenden Algorithmus (MD5 oder MD5-sess). Anhand der übermittelten Parameter berechnet der UAC aus Benutzername, Passwort, *Nonce*, SIP-Methode und *Request-URI* mit dem entsprechenden Algorithmus eine Prüfsumme. Diese Prüfsumme wird neben anderen Parametern, wie dem zugehörigen *Nonce*, in einer darauf folgenden erneuten Anfrage übermittelt.

```
Authorization: Digest username="snom",realm="asterisk",
nonce="369c5615",uri="sip:192.168.2.1",
response="e9a18b1089f0125d2c8b465c6aeb687b",algorithm=md5
```

Neben der Prüfung der Identität wird damit die SIP-Methode und die *Request-URI* zusätzlich vor Manipulation geschützt. Der SIP-Server berechnet ebenfalls die Prüfsumme und prüft diese gegen die von UAC übermittelten Werte. Bei einer positiven Prüfung wird dies durch die Statusmeldung `SIP/2.0 200 OK` bestätigt.

[14] [FHBH+99]

2.2.2 H.323

Der Standard H.323 wird von der ITU-T[15] entwickelt. Die erste Version des H.323-Standards wurde im Jahr 1996 veröffentlicht. Aktuell liegt die vorveröffentlichte Version 6 vor. Alle Versionen sind rückwärtskompatibel zu den Vorgängerversionen [IT06c].

H.323 ermöglicht die Übertragung von Echtzeitdaten wie Sprache, Video und Daten über paketbasierende Netzwerke, die keine Mechanismen zur Dienstgüte bereitstellen [IT06c]. H.323 gilt allgemein als zuweilen kompliziertes [Por06, S. 124] und sehr komplexes [AAG+05, S. 33] Protokoll. Dem unmittelbaren Konkurrent SIP wird hingegen ein wesentlich vereinfachter Aufbau zugesprochen [AAG+05, S. 19].

Zu den grundlegenden Komponenten der H.323-Architektur gehören die Komponenten Terminal, Gateway, Gatekeeper und Multipoint Control Unit (MCU), die in [IT06c, Kap. 6] beschrieben werden.

Terminals sind H.323-Endgeräte wie IP-Telefone und Softphones, mit denen Anrufe getätigt und entgegen genommen werden können[16]. Die Übertragung von Video und Daten zwischen Terminals wird im H.323-Standard als optional vermerkt. Zusätzlich wird neben Punkt-zu-Punkt-Verbindungen auch die Übertragung zwischen drei und mehr Teilnehmern in einer Multipunkt-Konferenz unterstützt.

Ein Gateway ist in einem H.323-Netzwerk eine optionale Komponente und wird nur benötigt, wenn die Signalisierung und Sprachübertragung zwischen unterschiedlichen Terminals ermöglicht werden soll. Dies kann die Kommunikation zwischen Terminals in unterschiedlichen paketbasierten VoIP-Netzwerken wie H.323 und SIP sein oder die Kommunikation zwischen Terminals in paketbasierten und leitungsvermittelnden Netzwerken wie H.323 und dem Public Switched Telefon Network (PSTN) [Por06, S. 125].

Wenn Terminals die IP-Adresse des Kommunikationspartners kennen, können diese direkt miteinander kommunizieren. Sollte dies nicht der Fall sein, ist der Einsatz von Gatekeepern erforderlich. Dabei übernimmt der Gatekeeper die Adressübersetzung zwischen einer H.323-Kennung und einer IP-Adresse, in dem eine Tabelle für alle registrierten H.323-Komponenten (*H.323 entities*) gepflegt wird. Die Funktionalität des Gatekeepers wird neben den Terminals auch von Gateways und MCUs genutzt. Zudem ermöglichen Gatekeeper die Verwaltung der Bandbreite, die Lokalisierung von Gateways sowie die Zugangskontrolle für H.323-Komponenten.

[15] Telecommunication Standardization Sector of the International Telecommunication Union (ITU)

[16] Das bekannteste Beispiel für ein H.323-Terminal, ist die Software Netmeeting der Firma Microsoft.

Um die beschriebene Funktionalität der Multipunkt-Konferenz bereitzustellen, wird eine sogenannte MCU benötigt, die die Verwaltung der Multipunktverbindung zwischen den Terminals und Gateways übernimmt.

Alle zuvor beschriebenen Komponenten, die durch einen Gatekeeper verwaltet werden, werden in der H.323-Terminologie als Zone bezeichnet. In jeder Zone existiert somit nur ein Gatekeeper. Durch die Funktionalität der Gateways existieren Zonen auch unabhängig von der jeweiligen Netzwerktopologie.

Im Folgenden sollen die VoIP-spezifischen Protokolle der H.323-Architektur erläutert werden. Eine Übersicht über die Protokolle und deren Zusammenhänge ist in Abbildung 2 dargestellt.

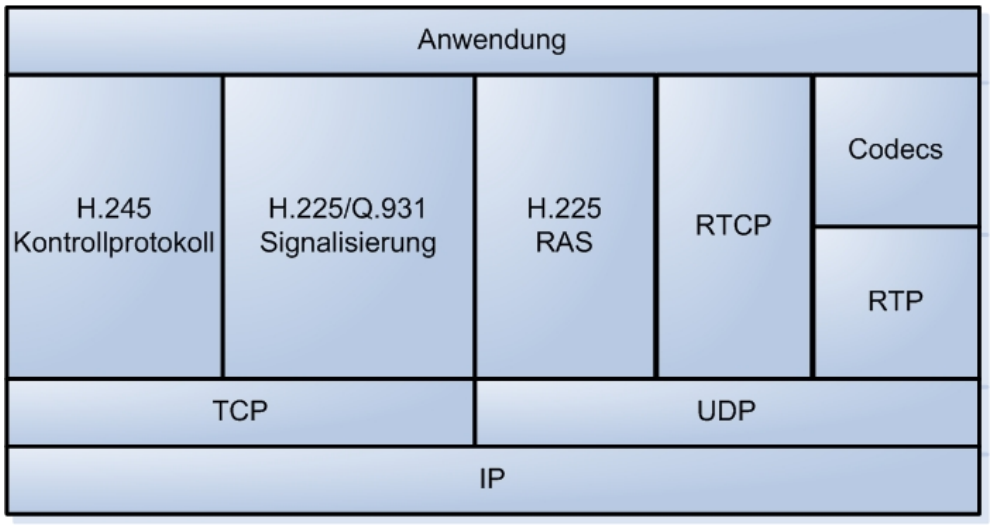

Abbildung 2: VoIP spezifischer H.323-Protokoll-Stack [Por06, S. 126]

Zur Signalisierung von Multimediadaten verwendet H.323 die Protokolle H.225[17] und H.245[18]. Zur Übertragung der Sprachdaten kommt das RTP und dessen Kontrollprotokoll Real Time Control Protocol (RTCP) zum Einsatz [SCFJ03].

Das H.225-Protokoll besitzt zwei verschiedene Einsatzmöglichkeiten. Zum einen ermöglicht es die Signalisierung der Gespräche auf Basis des ISDN D-Kanal Protokolls Q.931. Dazu gehört der Auf- und Abbau sowie die Kontrolle der Gesprächsverbindungen. Die Übertragung der H.225/Q.931-Nachrichten erfolgt zuverlässig über das TCP. Zum anderen ermöglicht RAS[19] innerhalb des H.225-Protokolls das Erkennen von Gatekeepern im Netzwerk durch einen *Multicast-Mechanismus*,

[17] [IT06a]
[18] [IT06b]
[19] Registration Admission and Status (RAS)

die Registrierung von H.323-Endgeräten, die Verwaltung der Bandbreite sowie den Austausch von Statusnachrichten. Im Gegensatz zu den H.225/Q.931-Nachrichten erfolgt der Transport der RAS-Nachrichten unzuverlässig über das UDP [Por06, S.126 ff.].

H.245 ist das Kontrollprotokoll, dessen Nachrichten zuverlässig über das TCP übertragen werden. Es ermöglicht das Öffnen und Schließen von logischen Kanälen, die für den Transport mit dem RTP genutzt werden. Zusätzlich werden Endgerätefunktionen (*Capabilities*), wie unterstütze Codecs, ausgetauscht [Por06; IT06c].

Die H.245-Nachrichten können auch in H.225-Nachrichten getunnelt werden, wodurch auf den Aufbau eines separaten H.245-Kanals verzichtet wird. Dieser Mechanismus ist ressourcenschonender und reduziert die Zeit für den Gesprächsaufbau [IT06c, Kap. 8.2.1]. Ein weitere Möglichkeit die Zeit für den Gesprächsaufbau bei H.323 zu reduzieren bietet der *Fast-Connect-Mechanismus*. Dabei werden die benötigten Nachrichten auf zwei innerhalb der H.225-Signalisierung reduziert [IT06c, Kap. 8.1.7]. In beiden Fällen kann jedoch die Übertragung auf einem separaten H.245-Kanal fortgesetzt werden, wenn die volle Funktionalität des H.245-Protokolls benötigt wird [IT06c, Kap. 8.2.3].

Anhand der Abbildung 3 soll der Kommunikationsablauf zwischen zwei H.323-Endgeräten über einen Gatekeeper vereinfacht[20] aufgezeigt werden. Grundlage für die Beschreibung des Protokolls sind die Dokumente [IT06a; IT06b; IT06c], die Software Netmeeting der Firma Mircosoft[21] sowie der GNU Gatekeeper (OpenH323 Gatekeeper)[22].

1. `H.225 - ARQ (RAS Control)`

   Der Aufbau der Gesprächsverbindung erfordert die vorherige Zugangskontrolle (*Admission Control*) durch den Gatekeeper. Ein Austausch der Nachrichten erfolgt während der Zugangskontrolle unter Verwendung des RAS-Protokolls. Die Genehmigung zum Verbindungsaufbau wird vom Terminal A (Alice) durch die ARQ-Nachricht[23] angefragt.

   Ebenfalls wird in dieser Nachricht die notwendige Bandbreite für Kommunikationsverbindungen (Audio) durch den Parameter *bandWidth* angefordert. Mit dem Parameter *destinationInfo* signalisiert Alice, dass sie Bob anrufen

[20] Vereinfacht bedeutet in diesem Zusammenhang, dass eine Registrierung der Terminals, der Abbau der Gesprächsverbindung sowie die Mechanismen zum schnellen Gesprächsaufbau nicht Bestandteil der Beschreibung ist. Weiterhin werden bei den Nachrichten nur für das Verständnis des Kommunikationsablaufs relevante Parameter erwähnt.

[21] http://www.microsoft.com/windows/netmeeting

[22] http://www.gnugk.org

[23] Admission Request (ARQ)

möchte. Dieser enthält die gewählte Nummer[24] oder die H.323-Kennung[25]. Im Folgenden wird von einer H.323-Kennung *bob* ausgegangen. Mit Hilfe des Parameters *srcInfo* gibt Alice ihre H.323-Kennung an. Zusätzlich werden noch Bezeichner übermittelt, die eine Zuordnung der Nachrichten und Verbindungen ermöglichen[26].

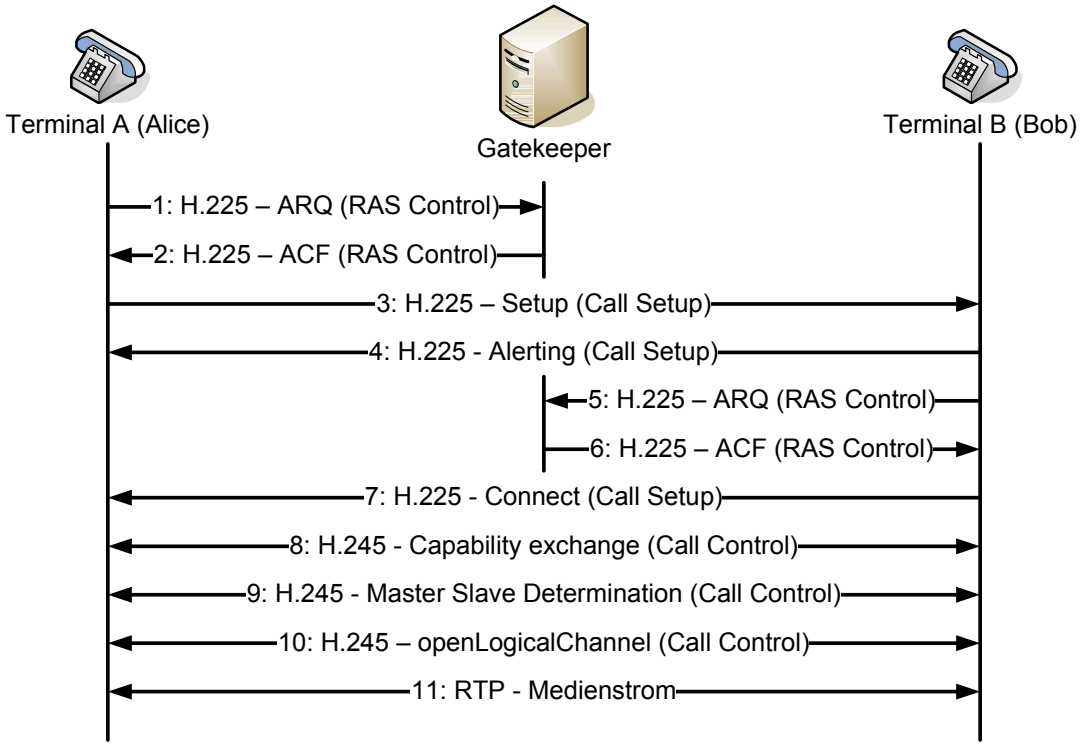

Abbildung 3: H.323-Kommunikation [IT06c]

2. `H.225 - ACF (RAS Control)`

   Der Gatekeeper besitzt nun die Möglichkeit den Zugang durch eine ARJ-Nachricht[27] abzulehnen oder durch Senden der ACF-Nachricht[28] zu gestatten (Abbildung 3) und Alice die Möglichkeit zu geben, den Gesprächsaufbau zu beginnen. Der Parameter *callModel* der ACF-Nachricht zeigt Alice an, ob die H.225-Nachrichten zur Signalisierung der Gespräche (*Call Setup*) direkt an den Gesprächspartner oder über den Gatekeeper geleitet werden. In dieser Beispielkommunikation arbeitet der Gatekeeper nicht im Modus *routed* und weist somit den Wert *direct* dem Parameter *callModel* zu.

[24] *dialedDigits*
[25] *h323-ID*
[26] *callReferenceValue*, *conferenceID* und *callIdentifier*
[27] Admission Reject (ARJ)
[28] Admission Confirmation (ACF)

Die für den Gesprächsaufbau notwendige Zieladresse (IP-Adresse und Port) wird im Parameter *destCallSignalAddress* übermittelt. In der ACF-Nachricht besteht für den Gatekeeper ebenfalls die Möglichkeit, die angeforderte Bandbreite zu reduzieren. Während der Verbindung können beide Kommunikationspartner zusätzlich eine Veränderung der Bandbreite initiieren[29].

3. `H.225 - Setup (Call Setup)`

   Mit der zuvor übermittelten Adresse des Terminals B (Bob) kann nun durch Senden der H.225-Nachricht *Setup* ein direkter Kanal zu Bobs Terminal aufgebaut werden. Der Parameter *srcInfo* enthält in diesem Fall nicht die H.323-Kennung, sondern einen *EndpointType*, über dessen Wert *terminal* Bob mitgeteilt wird, dass die Anfrage zum Rufaufbau von einem Terminal kommt und somit kein Gatekeeper an dem Gesprächsaufbau (*Call Setup*) beteiligt ist. Für den weiteren Ablauf der Kommunikation ist noch die Quelladresse notwendig, unter der Alice zu erreichen ist. Diese wird im Parameter *destCallSignalAddress* übermittelt.

4. `H.225 - Alerting (Call Setup)`

   Durch Senden der H.225-Nachricht *Alerting* wird dem Terminal von Alice signalisiert, dass die Anfrage zum Verbindungsaufbau das Terminal erreicht hat und Bob durch das Klingeln seines Terminals der Anruf angekündigt wird.

5. `H.225 - ARQ (RAS Control)`

   Bob fordert nun ebenfalls die Erlaubnis für den Zugang vom Gatekeeper an (siehe Schritt 1), wobei der Parameter *destinationInfo* weiterhin die Kennung von Bob enthält.

6. `H.225 - ACF (RAS Control)`

   Die Erlaubnis wird analog zu Schritt 2 durch die ACF-Nachricht erteilt.

7. `H.225 - Connect (Call Setup)`

   Durch die H.225-Nachricht *Connect* wird dem Terminal von Alice signalisiert, dass Bob den Anruf angenommen hat und zwischen den Terminals eine Verbindung besteht. Zusätzlich wird noch der Parameter *h245Address* übermittelt. Dieser gibt die Adresse an, unter der Bob den Aufbau des H.245-Kanals erwartet.

8. `H.245 - Capability exchange (Call Control)`

[29] Bandwidth Change Request (BRQ)

Der Austausch der Endgerätefunktionen (*Capability Exchange*) ermöglicht Alice und Bob mitzuteilen, welche Codecs sie für das Senden und Empfangen der Multimediadaten unterstützen (*terminalCapabilitySet*). Der erfolgreiche Empfang der Endgerätefunktionen wird vom jeweiligen Terminal durch die H.245-Nachricht *terminalCapabilitySetAck* bestätigt.

9. `H.245 - Master Slave Determination (Call Control)`

   Da während des Verbindungsaufbaus keine Synchronisation und kein Sperrmechanismus existiert, kann es passieren, dass zwei Terminals versuchen, zur gleichen Zeit einen logischen Kanal für die Sprachübertragung zu öffnen. Um solche Konflikte zu vermeiden, kommt ein sogenannter *Master-Slave-Mechanismus* zum Einsatz. Dieser wird durch eine Anfrage vom Typ *masterSlaveDetermination* initiiert. Dabei werden zwei Nummern übermittelt, eine vom Typ *terminalType* und eine vom Typ *statusDeterminationNumber*. Das Terminal, welches die Anfrage erhält, vergleicht die Nummer vom Typ *terminalType* mit der eigenen und das Terminal mit der höchsten Nummer wird Master-Terminal. Sollte der Wert gleich sein, entscheidet die Wertigkeit der *statusDeterminationNumber*. Das Ergebnis der Berechnung wird dem Kommunikationspartner in einer Antwort vom Typ *masterSlaveDeterminationAck* übermittelt. Dort wird im Parameter *decision* angeben, ob er *Master-* oder *Slave-Terminal* ist.

10. `H.245 - open Logical Channel (Call Control)`

    Den Aufbau von zwei logischen Kanälen zwischen den beiden Terminals, wie sie für den Transport der Sprachdaten (RTP) und dessen Kontrollnachrichten (RTCP) benötigt werden, initiiert die H.245-Nachricht *openLogicalChannel*. Dabei beschreibt *openLogicalChannel* die Kanäle mit Parametern wie *audioData*, der den verwendeten Codec angibt. Ein weiterer Parameter ist *iPAddress*, welcher die IP-Adresse[30] und den Port[31] für die RTCP-Verbindung angibt, auf der Alice's Terminal die Verbindungsanfrage erwartet.

    Die H.245-Nachricht *openLogical-ChannelAck* schließt die Verhandlung der Parameter für die Sprachübertragung ab, indem sowohl die für den Aufbau der RTP-Verbindung als auch die für die RTCP-Verbindung notwendige Adresse (IP-Adresse und Port) an Alice Terminal übermittelt wird. Die aufgebauten logische Kanäle sind uni-direktional, folglich müssen insgesamt 4 Kanäle etabliert werden [KWF05, S. 28]. Daraus resultiert, dass die zwei Nachrichten zum Aufbau der RTP- und RTCP-Verbindung für jede Übertragungsrichtung gesendet werden müssen.

[30] *network*
[31] *tsapIdentifier*

11. `RTP - Medienstrom`

    Nun können die Multimediadaten zwischen den beiden Terminals über das RTP ausgetauscht werden. Eine Beschreibung der Funktionsweise des RTP erfolgt in Kapitel 2.2.4.

2.2.3 SCCP

Das Skinny Client Control Protocol (SCCP) ist ein proprietäres Protokoll der Firma „Cisco“ zur Signalisierung von Sprachverbindungen. In der Literatur wird SCCP auch verkürzt *Skinny* genannt und wurde ursprünglich von der Firma „Selsius Corporation“ entwickelt, die von Cisco übernommen wurde. Das SCCP ist nicht offengelegt und wird somit vorwiegend in Cisco-Produkten eingesetzt. Dort ermöglicht es die Umsetzung individueller Leistungsmerkmale, die besonders für Firmen interessant sind. Eine VoIP-Installation unter Verwendung des SCCP beinhaltet neben den Endgeräten auch einen sogenannten *Call-Manager*. Neben der Zugangskontrolle und Vermittlung der Gespräche ermöglicht dieser auch die Kommunikation in andere VoIP-Netzwerke, in denen die Endgeräte das SCCP nicht umsetzen. Die Übertragung der Signalisierungsnachrichten erfolgt dabei binär codiert unter Verwendung des TCP. Für die Übertragung der Sprachdaten kommt beim SCCP ebenfalls das RTP zum Einsatz [Por06, S. 231 ff.].

2.2.4 RTP & RTCP

Das Real-Time Transport Protocol (RTP) wird in RFC 3550[32] spezifiziert und löst das im Jahr 1996 standardisierte RFC 1889 ab. Es ermöglicht die Ende-zu-Ende-Übertragung von Multimediadaten mit Echtzeiteigenschaften, wie bei der Sprache oder einem Video [SCFJ03]. Für den Einsatz bei VoIP wird im Folgenden von einer Übertragung von Sprachdaten gegenüber Multimediadaten (Video und Audio) ausgegangen. Dabei wird das RTP von mehreren Signalisierungsprotokollen (SIP, H.323 und SCCP) für die Übertragung der Sprachdaten verwendet.

Neben der einfachen Übertragung von *Unicast-Datenströmen* zwischen einzelnen Teilnehmern ermöglicht das RTP zusätzlich die Übertragung von Datenströmen in *Multicast-Umgebungen* und somit die Realisierung von Konferenzen. Jedoch stellt es keine Mechanismen zum Auf- und Abbau einer Sprachverbindung bereit. Dies ist durch Signalisierungsprotokolle wie dem SIP und H.323 (H.224 und H.225) sicherzustellen.

Für die Übertragung der Sprachpakete baut das RTP üblicherweise auf dem verbindungslosen und unzuverlässigen UDP auf [SCFJ03, Kap. 1]. Eine Verhandlung der vom RTP verwendeten Ports erfolgt jeweils durch das eingesetzte Signalisierungsprotokoll. Zusätzlich muss im Rahmen der Signalisierung zwischen den

[32] [SCFJ03]

Kommunikationspartnern die Kompatibilität der eingesetzten Codecs gewährleistet werden. Diese Aufgabe kann von einem Protokoll wie SDP übernommen werden, welches eine Vereinbarung der eingesetzten Codecs[33] und den Austausch von Parametern zum Aufbau der Sprachverbindung ermöglicht (siehe Kapitel 2.2.1).

Ein RTP-Paket besteht aus einem *RTP-Header* und der RTP-Nutzlast (*RTP-Payload*). Während der *RTP-Header* zusätzliche Informationen zur Verwaltung einer RTP-Sitzung (*RTP-Session*) bereitstellt, enthält der *RTP-Payload* die übertragenen Sprachpakete. Die zur Übertragung der Nutzdaten wesentlichen Informationen des *RTP-Headers* werden im Folgenden genannt [AAG+05; SCFJ03].

- Payload Type (PT): Der *Payload-Typ* bezeichnet den zur Codierung der Sprachdaten verwendeten Codec[34].
- Timestamp: Der Zeitstempel dient der Synchronisation der Nutzdaten.
- Sequence Number: Die Sequenznummer ermöglicht es, die korrekte Reihenfolge von aufeinander folgenden RTP-Paketen mit unterschiedlichen Übertragszeiten beim Empfänger wiederherzustellen. Durch die fortlaufende Nummerierung lassen sich mögliche Paketverluste während der Übertragung feststellen.
- Synchronisation Source (SSRC) Identifier: Der SSRC-Bezeichner ermöglicht die Identifikation einer Datenquelle (SSRC) innerhalb einer RTP-Sitzung. Somit lassen sich zusammengehörige RTP-Pakete einer Quelle zur Wiedergabe gruppieren.
- Contributing Source (CSRC) List: Die CSRC-Liste ermöglicht die Identifizierung mehrerer Datenquellen (SSRC) einer RTP-Sitzung, wenn diese durch ein zusätzliches Gerät (Mixer) zu einer Datenquelle gemischt werden und somit alle RTP-Pakete den SSRC des Mixers enthalten.

Die Kontrolle der Echtzeitkommunikation beim RTP erfolgt durch das RTCP, das Kontroll- und Statusinformationen des aktuellen RTP-Datenstroms für alle teilnehmenden Kommunikationspartner zur Verfügung stellt. Somit stellt RTCP neben den Informationen über die Teilnehmer einer RTP-Sitzung zusätzlich Informationen zur Qualität einer RTP-Sitzung bereit. Jedoch bietet das RTP keinen Mechanismus an, um eine bestimmte Dienstgüte (QoS) zu garantieren. Weiterhin wird im Standard nicht spezifiziert, wie mit Schwankungen in der Übertragungszeit (Jitter) und mit Paketverlusten umgegangen werden soll. Die Übertragung

[33] Die Verhandlung der eingesetzten Codecs kann anhand der Abbildung 4 nachvollzogen werden.

[34] Mögliche Codecs können zum Beispiel G.711 aLaw mit 64 kbit/s Bitrate oder G.729 mit 8 kbit/s Bitrate sein

der Kontroll- und Statusinformationen erfolgt bei RTCP durch vier verschiedene Pakettypen, deren Funktion im Folgenden erläutert werden soll [SCFJ03].

- Sender Report 200 (SR 200)

  Ein SR beinhaltet Berichte über empfangene und gesendete Daten von aktiven Sendern und ermöglicht dem Empfänger, Rückschlüsse auf die Dienstgüte der Übertragung zu ziehen.

- Receiver Report 201 (RR 201)

  Ein RR beinhaltet Berichte über empfangene Daten von reinen Empfängern.

- Source Description 200 (SDES 202)

  In einem SDES-Paket ist es möglich, zusätzliche Informationen über eine Quelle (SSRC) zu schicken.

- BYE 203

  Ein BYE-Paket signalisiert den anderen Kommunikationsteilnehmern, dass die Quelle (SSRC) nicht länger zur Verfügung steht.

- APP 204

  Das APP-Paket ist für experimentelle Zwecke wie neuen Eigenschaften und neuen Anwendungen vorgesehen.

Wie in der beispielhaften SIP/RTP-Sitzung[35] in Abbildung 4 zu sehen ist, werden bei der Nutzung des RTP im Zusammenhang mit VoIP jedoch lediglich die Pakettypen SR und BYE verwendet. Der Pakettyp RR entfällt, da bei der Kommunikation über VoIP nur aktive Sender (SR) auftreten.

RTP und RTCP bilden zusammen eine RTP-Sitzung (siehe Abbildung 4). Die Anzahl der *Streams* in einer RTP-Sitzung kann je nach Anzahl der Kommunikationsteilnehmer, beispielsweise bei einer Konferenzschaltung, variieren. Die Übertragung von Multimediadaten würde pro Medium in einer separaten Sitzung erfolgen.

[35] In Abbildung 4 wurde auf die Darstellung von SIP-Statusnachrichten verzichtet.

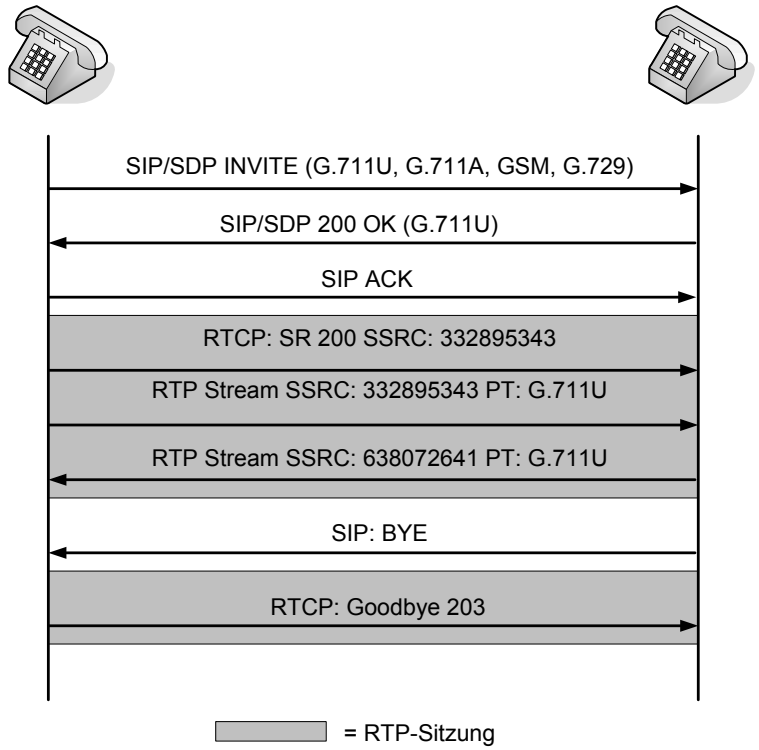

Abbildung 4: Beispielablauf einer SIP/RTP-Sitzung

2.2.5 SRTP

Das Secure Real-time Transport Protocol (SRTP) ist eine Erweiterung für das RTP und dessen Kontrollprotokoll RTCP, welches in RFC 3711[36] definiert wird. Es dient der Sicherstellung von Vertraulichkeit, Authentifikation und Integrität der Sprachverbindung. Zusätzlich bietet das SRTP einen Schutz vor *Reply-Angriffen* [BMN+04].

Als Verschlüsselungsalgorithmus wird der Advanced Encryption Standard (AES)[37] in zwei verschiedenen Modi (Counter-Mode[38] und f8-Mode) eingesetzt. Allerdings ist der f8-Mode in [BMN+04] als optional gekennzeichnet und für die Verschlüsselung von UTMS vorgesehen. Zur Vollständigkeit soll auch die *NULL-Chiffre* erwähnt werden, die eingesetzt wird, wenn keine Vertraulichkeit zwischen den Kommunikationspartnern bestehen muss [BMN+04].

Das SRTP setzt die zwei verschiedenen Schlüsselarten Master- und Sitzungsschlüssel ein. Dabei gilt es, den Masterschlüssel auf gesicherte Weise auszutau-

[36] [BMN+04]

[37] Als symmetrischer Verschlüsselungsalgorithmus ist der AES aufgrund seiner Performance bestens für die Verschlüsselung von zeitkritischen Protokollen wie dem RTP geeignet.

[38] Der Counter-Mode wird in der Fachliteratur mit AES-CM oder AES-CTR abgekürzt.

schen, so dass daraus die zur Verschlüsselung (128 Bit) oder Authentifikation (160 Bit) eingesetzten Sitzungsschlüssel durch eine kryptografisch sichere Funktion abgeleitet werden können. Eine Verwaltung und ein sicherer Austausch des benötigten Schlüsselmaterials ist jedoch nicht Bestandteil des Protokolls und muss durch ein zusätzliches Schlüsselmanagementprotokoll sichergestellt werden (siehe Kapitel 2.2.9 Sicherer Schlüsselaustausch) [BMN+04].

Ein SRTP-Paket besitzt den gleichen Header wie ein herkömmliches RTP-Paket mit dem Unterschied, dass durch zwei zusätzliche Felder (Master Key Identifier (MKI), *Authentication Tag*) der MKI, der den verwendeten Masterkey für das jeweilige RTP-Paket bestimmt, und die Prüfsumme des RTP-Paketes übertragen werden können [BMN+04].

Die Verschlüsselung in den beiden Modi AES-CM und AES-f8 erfolgt durch bitweise *XOR-Verknüpfung* der RTP-Nutzlast mit dem zum RTP-Paket erzeugten pseudo-zufälligen Schlüsselstrom. Wie der Schlüsselstrom erzeugt wird, hängt von den eingesetzten Modi ab. Im Counter-Modus (AES-CM) wird der Schlüsselstrom durch die Konkatenation von 128 Bit Block-Chiffren erzeugt. Diese werden durch die Chiffrierung eines Sitzungsschlüssels, eines Initialisierungsvektors IV und eines Blockindizes erzeugt [BMN+04; AAG+05].

Die Authentifikation der RTP-Pakete wird beim SRTP durch die *Hashfunktion* HMAC-SHA1 sichergestellt. Dabei wird der erzeugte *Hashwert* (160 Bit), der zusätzlich die Integrität des *RTP-Headers* und der RTP-Nutzlast sicherstellt, an das Ende des RTP-Paketes angehängt (*Authentication Tag*) [BMN+04].

Der im SRTP eingesetzte *Reply-Schutz* arbeitet mit einer *Reply-Liste* und einem definierten Zeitfenster. Die *Reply-Liste* enthält alle Indices der Pakete, die bereits empfangen und authentifiziert wurden. Somit wird jeder Index eines Paketes gegen die *Reply-Liste* und das Zeitfenster geprüft. Ein Paket wird nur zugelassen, wenn der Index innerhalb oder vor dem Zeitfenster liegt und nicht in der *Reply-Liste* aufgeführt ist [BMN+04].

2.2.6 H.235

H.235 definiert Sicherheitsfunktionen zur sicheren Übertragung der Signalisierung (H.225[39] und H.245[40]) und der Sprachdaten (RTP) bei H.323. Dabei soll dafür Sorge getragen werden, dass ein Abhören sowie das Manipulieren der Signalisierung und der Sprachdaten nicht möglich ist. H.235 kann folglich beim Einsatz der H.323-Architektur Authentifikation, Privatsphäre und Integrität für die übertragenen Daten sicherstellen [IT00].

Seit 2005 liegt H.235 in der Version 4 vor (H.235v4 [IT05a]). H323v1 wurde im Jahr 1998 veröffentlicht. H.235v2 aus dem Jahr 2000 erweitert H.235v1 um Kryptographie basierend auf elliptischen Kurven, dem Verschlüsselungsalgorithmus AES[41] und einem Mechanismus, der es dem Empfänger erlaubt RTP-Pakete zu erkennen, die von einer unautorisierten Quelle in den RTP-Strom eingefügt werden (*Media Anti-Spamming*). Zusätzlich wurden Sicherheitsprofile eingeführt, welche die Interoperabilität zwischen den H.323-Produkten erhöhen sollen [IT00].

Durch die Spezifikation H.235v3 aus dem Jahr 2003 wird die H.323-Architektur um die Möglichkeit der Verschlüsselung von DTMF-Tönen[42] erweitert, um Parameter für die Verschlüsselung der RTP-Nutzlast durch AES sowie den zusätzlichen Betriebsmodus EOFB[43], der die bitweise Verschlüsselung (Stromchiffre) der Sprachdaten ermöglicht. Zusätzlich wird eine Option (*Authentication-Only*) definiert, welche die Authentizität nur auf ausgewählte Felder einer Nachricht beschränkt und auf eine Sicherstellung der vollen Integrität der Nachrichten verzichtet, um somit eine reibungslose Übertragung über NAT-Grenzen[44] hinweg zu ermöglichen. Weitere Neuerungen sind ein erweitertes Schlüsselmanagement sowie eine zusätzliche Unterstützung von Sicherheitsmaßnahmen bei einer direkten Anrufsignalisierung [IT00; AAG+05].

Der Inhalt des H.235-Standards (H.235v3) wurde im Rahmen der Standardisierung von H.235v4 auf sieben verschiedene Standards verteilt (H.235.x), die den H.235-Sicherheitsprofilen der Version H.235v3 entsprechen. Weiterhin wurden die Sicherheitsprofile H.235.8 und H.235.9 hinzugefügt und die Profile H.235.3 und H.235.5 um zusätzliche Funktionalität erweitert. Dabei bildet H.235.0 das Rahmendokument mit einer allgemeinen Beschreibung der bereitgestellten Sicherheitsfunktionen. Die Umsetzung der einzelnen Sicherheitsprofile ist optional. H.323-Produkte können somit vereinzelte oder alle Sicherheitsprofile umsetzen. Um die sichere Kommunikation zwischen den Produkten zu ermöglichen,

[39] RAS-Signalisierung und Anrufsignalisierung
[40] Signalisierung des Steuerungskanals
[41] Advanced Encryption Standard (AES)
[42] DTMF-Töne ermöglichen im Rahmen des Tonwahlverfahrens eine Übertragung der gewählten Ziffern zum Gesprächspartner.
[43] Enhanced Output Feedback Mode (EOFB)
[44] Network Address Translation (NAT)

erfolgt innerhalb der Registrierung eine Verständigung gegenüber dem Gatekeeper (*Offer/Answer-Mechanismus*) auf die in der Kommunikation verwendeten Sicherheitsprofile. Die H.235-Spezifikation gibt dabei vor, welche Sicherheitsprofile gleichzeitig genutzt werden können [IT05a, S. 13]. Eine Übersicht über die Sicherheitsprofile in H.235v4 liefert die Tabelle 2.

Sicherheitsprofile	Einführung
235.1 Baseline Security Profile	H.235v2
235.2 Signature Security Profile	H.235v2
235.3 Hybrid Security Profile	H.235v2
235.4 Direct and Selective Routed Call Security	H.235v3
235.5 Framework for secure authentication in RAS using weak shared secrets	H.235v3
235.6 Voice encryption profile with native H.235/H.245 key management	H.235v2
235.7 MIKEY + SRTP security profile	H.235v3
235.8 Key Exchange for SRTP using secure Signalling Channels	H.235v4
235.9 Security Gateway Support for H.323	H.235v4

Tabelle 2: Sicherheitsprofile in H.235

Das *Baseline Security Profile* (H.235.1), das *Signature Security Profile* (H.235.2) sowie das *Hybrid Security Profile* (H.235.3) definieren Sicherheitsmechanismen für die Signalisierung durch die Protokolle RAS, H.225/Q.931 und H.245[45]. Diese Profile unterstützen die bereits erwähnte Option *Authentication-Only*, die nur die Authentizität bestimmter Nachrichtenfelder sichergestellt, wodurch einige Felder im Rahmen des NAT verändert werden können [IT00].

Das *Baseline Security Profile* basiert auf symmetrischer Kryptographie. Die Authentizität und Integrität der Nachrichten wird durch einen gemeinsamen geheimen Schlüssel (*Shared Secret*) und den Einsatz des *Hash-Algorithmus HMAC-SHA1-96* sichergestellt [IT05b, Kap. 6].

Durch den Einsatz symmetrischer Verschlüsselung bietet H.235.1 nur *Hop-by-Hop-Sicherheit* für die Signalisierungsnachrichten an, kann dadurch jedoch die Authentizität und Integrität der ganzen Nachricht sicherstellen [IT05b, Kap. 3.2].

Das *Signature Security Profile* basiert auf asymmetrischer Verschlüsselung (Public-Key-Verschlüsselung). Anhand von Zertifikaten und Signaturen ermöglicht dieses Sicherheitsprofil neben Nicht-Abstreitbarkeit und Integrität, auch die

[45] Die H.245-Nachrichten werden dabei innerhalb der Anrufsignalisierung durch H.225 übertragen und nicht in einer separaten Verbindung (*H.245 tunneling*).

Hop-by-Hop- und Ende-zu-Ende-Authentifizierung sicherzustellen. Es stellt folglich eine Erweiterung bezüglich der Sicherheit gegenüber dem *Baseline Security Profile* dar und eine gleichzeitige Nutzung beider Profile ist somit nicht möglich.

Beim Einsatz der Signaturen kann zwischen *RSA-SHA-1* und *RSA-MD5* gewählt werden. *Public-Key-Verfahren* eignen sich besser für große Umgebungen, da eine Verwaltung des Schlüsselmaterials durch eine Public Key Infrastruktur (PKI) wesentlich effizienter gestaltet werden kann. Hingegen kann sich die aufwendige Signatur und Verifikation der Nachrichten nachteilig auf die Performance auswirken, sollte die Rechenleistung der Endgeräte nicht ausreichend dimensioniert sein [IT05c; KWF05].

Das *Hybrid Security Profile*[46] vereint das *Baseline Security Profile* und das *Signature Security Profile*, in dem sowohl symmetrische als auch asymmetrische Kryptographie in Verbindung mit einer PKI zum Einsatz kommen. Durch den Einsatz einer PKI eignet sich das hybride Sicherheitsprofil gegenüber dem *Baseline Security Profile* wesentlich besser für den Einsatz in großen Umgebungen. Zusätzlich wird zugunsten der Performance darauf verzichtet, dass für alle Nachrichten digitale Signaturen zum Einsatz kommen und somit keine hohen Anforderungen an die Rechenleistung der Endgeräte gestellt werden. Digitale Signaturen kommen nur beim ersten *Handshake* zwischen den Kommunikationspartnern zum Einsatz. Innerhalb dieses *Handshakes* wird zusätzlich ein Diffie-Hellmann-Schlüsselaustausch ausgeführt. Ein daraus resultierender gemeinsamer geheimer Schlüssel, wird wie beim *Baseline Security Profile* für die Authentizität und Integrität der nachfolgenden Signalisierungsnachrichten eingesetzt [IT05d]. Gegenüber dem *Signature Security Profile* wird auf den Einsatz von *RSA-MD5* verzichtet[47]. Als möglichen Grund dafür nennt die BSI-Studie VoIPSEC [AAG+05, S. 109] die erfolgreichen Kollisionsangriffe auf MD5, welche „*die benötigte Komplexität deutlich verringern*“.

Das Sicherheitsprofil *Direct and Selective Routed Call Security* (H.235.4[48]) erweitert die Sicherheitsmechanismen bei einer direkten Anrufsignalisierung für das *Baseline Security Profile* und das *Hybrid Security Profile*. Charakteristisch für dieses Modell ist, dass lediglich RAS-Nachrichten zwischen den H.323-Komponenten und dem Gatekeeper ausgetauscht werden und der Gesprächsaufbau direkt zwischen den Kommunikationsteilnehmern erfolgt[49]. Problematisch in diesem Modell ist die Verteilung der Schlüssel, da bei der direkten Anrufsignalisierung der Gatekeeper als vertrauenswürdige Zwischeninstanz nicht zur Verfügung steht und somit auch kein *Pre-Shared-Key* in Form eines Passwortes vorausgesetzt werden kann. Um den Kommunikationspartnern dennoch einen Sitzungsschlüssel

[46] [IT05d]
[47] „*RSA certificates with MD5 hashing are not part of this security profile.*“ [IT00, S. 91]
[48] [IT05e]
[49] Der Kommunikationsablauf in Abbildung 3 im Kapitel 2.2.2 erfolgt beispielsweise nach dem Modell der direkten Anrufsignalisierung.

für die Anrufsignalisierung bereitzustellen, übernimmt der Gatekeeper die Rolle eines Key-Distribution-Centers wie sie im Kerberosprotokoll (RFC 4120) definiert ist [AAG+05, S. 104]. Dies kann sowohl auf eine H.323-Zone angewandt werden als auch auf mehrere, die sich sowohl in unterschiedlichen als auch gleichen administrativen Domänen mit entsprechenden Sicherheitsrichtlinien befinden können [IT05e].

Innerhalb der RAS-Signalisierung ermöglicht der Standard H.235.5[50] eine stärkere Authentifizierung bei der Verwendung eines gemeinsamen Geheimnisses, wie einem Passwort. Ziel des Standards ist es, Angriffe auf kryptografisch schwache Passwörter (*Brute-Force*- und Wörterbuch-Angriffe) zu vermeiden, indem das Passwort zusammen mit symmetrischer Verschlüsselung und dem kryptografisch starken Diffie-Hellman-Verfahren eingesetzt wird. Zusätzlich kann ein abgeleiteter geheimer Schlüssel genutzt werden, um Sitzungsschlüssel für eine Verschlüsselung durch Transport Layer Security (TLS) bereitzustellen [IT05f].

Das *Voice Encryption Profile* (H.235.6[51]) stellt Mechanismen zum Schlüsselmanagement, zur Schlüsselerneuerung und zur Verschlüsselung des RTP bereit. Somit ermöglicht H.235.6 zusätzlich zur sicheren Signalisierung durch die Profile H.235.1, H.235.2 und H.235.3 die Vertraulichkeit der Sprachdaten sicherzustellen. Außerdem wird in H.235.6 die Verschlüsselung der DTMF-Töne spezifiziert. Mögliche Verschlüsselungsalgorithmen sind AES, RC2, DES oder 3-DES. Dabei sollen die Varianten 56-bit DES und 56-bit RC2 ausschließlich eingesetzt werden, um beispielsweise kompatibel zu den Standards H.235v2 und H.235v3 zu sein. Zur Ende-zu-Ende-Schlüsselvereinbarung wird das Diffie-Hellman-Verfahren eingesetzt. Der daraus abgeleitete Schlüssel wird zum sicheren Austausch der *Session-Keys* eingesetzt, welche zur Verschlüsselung der RTP-Sitzung verwendet werden [IT05g].

Das Profil H.235.7[52] beschreibt die Verwendung des Schlüsselmanagementprotokolls MIKEY[53] in Verbindung mit SRTP. Dabei realisiert MIKEY die Ende-zu-Ende-Verteilung der Schlüssel und Sicherheitsparameter zwischen den Kommunikationspartnern. Der H.235-Standard ermöglicht mit der Spezifikation von H.235.7 neben erhöhter Sicherheit auch die Interoperabilität mit SIP-Endgeräten herzustellen, die ebenfalls SRTP und MIKEY umsetzen. Zusätzlich soll mit H.235.7 auch dem Bedarf gerecht werden, ein Schlüsselmanagement ohne den Einsatz einer PKI zu ermöglichen. Dabei definiert H.235.7 zwei Profile, die zum einen auf symmetrischer als auch auf asymmetrischer Kryptographie beruhen. Wird das Profil mit asymmetrischer Kryptographie und einer entsprechenden PKI eingesetzt, hat dies den Vorteil, dass der Austausch der Schlüssel für SRTP

[50] "Framework for secure authentication in RAS using weak shared secrets" [IT05f]
[51] [IT05g]
[52] [IT05h]
[53] Multimedia Internet KEYing (MIKEY)

Ende-zu-Ende erfolgt und ein Abhören durch beteiligte Netzkomponenten vermieden wird [IT05h].

Das Profil 235.8[54] erweitert H.235 um Verfahren und Parameter zur Bereitstellung von Schlüsselmaterial für das SRTP über einen sicheren Kanal. Dieser kann durch den Einsatz von Protokollen wie IPSec[55] oder TLS bereitgestellt werden. Dabei sollen die Verfahren nicht eingesetzt werden, wenn der sichere Kanal an einem dazwischenliegenden Netzknoten terminiert wird. Für diesen Fall spezifiziert 235.8 ein zusätzliches *Public-Key-Verfahren*, bei dem der Ende-zu-Ende-Transport des Schlüsselmaterials durch vorherige Verschlüsselung und anschließende Signatur sichergestellt wird. Der Einsatz von 235.8 ist jedoch auf eine Punkt-zu-Punkt-Verbindung beschränkt [IT05i].

Der *Security Gateway Support* für H.323 im Standard 235.9[56] soll die in den Standards 235.1, 235.2, 235.3 und 235.5 beschrieben Sicherheitsmechanismen auch in Szenarien ermöglichen, bei denen durch den Einsatz eines Application Layer Gateways (ALG) einzelne Felder und Adressen verändert werden. Dazu wird in 235.9 eine Methode definiert, mit dessen Hilfe ein ALG im Signalisierungspfad erkannt wird und diesem ebenfalls der notwendige Schlüssel zur Authentifikation bereitgestellt werden kann. Somit kann der ALG notwendige Veränderungen vornehmen und diese anschließend gültig authentifizieren [IT05j].

2.2.7 IAX2

Die Abkürzung IAX2 steht für das Inter-Asterisk eXchange Protokoll[57] in der Version 2 und soll im folgenden Kapitel auf Grundlage der Dokumente [SCG+06] und [Por06, S. 195 ff.] beschrieben werden. IAX ist ein *Peer-to-Peer-Protokoll*[58], das vorwiegend in der Open-Source IP-Telefonanlage Asterisk zum Einsatz kommt. Neben der Kommunikation zwischen zwei Asterisk IP-Telefonanlagen existieren auch Endgeräte, wie Hardware- oder Software-Clienten, die Gespräche auf Basis des IAX-Protokolls ermöglichen.

IAX ist in erster Linie für die Signalisierung und Übertragung von Sprachdaten ausgelegt, kann jedoch anstatt der Sprachdaten ebenso für den Transport von Multimediadaten (Audio und Video) genutzt werden. Es ist somit das einzige offen gelegte Protokoll, welches die Signalisierung und Übertragung der Sprachdaten innerhalb einer Protokollarchitektur realisiert. Dies ermöglicht, einen stati-

[54] „Key exchange for SRTP using secure signalling channels“ [IT05i]
[55] Internet Protocol Security (IPSec)
[56] [IT05j]
[57] [SCG+06]
[58] Voraussetzung für die *Peer-to-Peer-Kommunikation* ist, dass beide Verbindungen (*call legs*) zu einem *Peer* das IAX-Protokoll unterstützen. Der *Peer* in der Mitte muss ebenfalls erkennen, dass er für die Kommunikation nicht benötigt wird und dann die Kommunikationsverbindung verlassen [SCG+06].

schen UDP-Port (4569) für die Signalisierung und den Transport der Sprachdaten zu verwenden. Somit reduziert IAX den *Overhead* gegenüber einer Realisierung, bei der die Übertragung der Signalisierung und der Sprachdaten durch zwei verschiedene Protokolle erfolgt. Der geringere *Overhead* und die binär codierte Übertragung der IAX-Nachrichten ermöglichen eine effektivere und damit sparsamere Nutzung der Bandbreite.

Zusätzlich werden Sprachverbindungen beim Einsatz von IAX in einer Verbindung gebündelt (*Trunking*). Dabei werden in einem *Trunk* die Nutzdaten einer oder mehrerer Sprachverbindungen unter Verwendung eines *Trunk-Headers* transportiert. Dies ermöglicht es, die zur Verfügung stehende Bandbreite effektiver zu nutzen, da die Anzahl der versendeten Pakete pro Verbindung und somit der *Overhead* durch zusätzliche *Header* reduziert werden kann.

Der Transport der IAX-Nachrichten in einer einzelnen Verbindung erleichtert die Übertragung der Sprachdaten über Netzwerkgrenzen mit NAT und Firewall. Damit ist ein *parsen* der Signalisierungsnachrichten nicht notwendig, da eine Vereinbarung der für die Übertragung der Sprachdaten verwendeten Ports innerhalb der Signalisierung entfällt. Firewallregeln können so wesentlich genauer und ohne den Einsatz eines ALG definiert werden, wodurch sich die Sicherheit gegenüber einem nicht vertrauenswürdigen Netzwerk erhöht.

IAX verwendet zur Adressierung von Kommunikationsteilnehmern einen ähnlichen Aufbau der URI, wie dies bei SIP der Fall ist, allerdings mit der notwendigen Unterscheidung im verwendeten protokollspezifischen Schemata (*iax2*). Der schematische Aufbau einer IAX-URI ist im Folgenden aufgezeigt.

```
iax2:benutzer@hostname
```

Die Übertragung der IAX-Nachrichten erfolgt in sogenannten *Frames*. Dabei wird zwischen *Full Frames* (12 Byte), *Mini Frames* (4 Byte) und *Meta Frames* unterschieden. Während in *Mini Frames* ausschließlich Sprach- bzw. Mediendaten übertragen werden, erfolgt innerhalb der *Full Frames* eine Übertragung der Signalisierungsnachrichten[59]. *Meta Frames* ermöglichen die Übertragung von *Trunk*- sowie Videoverbindungen (*Meta Trunk Frames* und *Meta Video Frames*).

Zusätzlich erfolgt innerhalb der Spezifizierung von IAX eine Unterscheidung zwischen zuverlässigem und unzuverlässigem Transport. Der Transport der *Full Frames* (Signalisierung) erfolgt zuverlässig, wohingegen *Mini* und *Meta Frames* unzuverlässig übertragen werden. Unzuverlässig bedeutet in diesem Fall, dass keinerlei Bestätigung über den erfolgreichen Empfang einer Nachricht versendet wird, während bei *Full Frames* eine Bestätigung durch ein *ACK* oder eine zum versendeten Frame Bezug nehmende Nachricht erfolgt.

[59] Neben der Übertragung der Signalisierungsnachrichten im *Meta Frame* ist auch die Übertragung von Mediendaten möglich. Dies verursacht jedoch aufgrund des zusätzlichen Versandes von Bestätigungen pro Frame und des größeren *Headers* gegenüber dem *Mini Frame* einen wesentlich höheren *Overhead*.

Bevor ein Kommunikationsteilnehmer für andere Teilnehmer erreichbar ist[60], muss sich dieser (*Registrant*) gegenüber dem *Registrar* anmelden. Zur Registrierung ist eine Authentifizierung notwendig. Die IAX-Spezifikation sieht dafür die drei Methoden *plain*, *md5* und *rsa* vor. Bei der Methode *plain* erfolgt eine Authentifizierung im Klartext und sollte somit nicht verwendet werden. Bei der Verwendung von *md5* erfolgt eine Übertragung des Passwortes auf Basis eines *Challenge-Response-Verfahrens* unter der Verwendung von *MD5-Hashverfahren*. Wird *rsa* eingesetzt, werden die Benutzerdaten auf Basis von *Public-Key-Verfahren* verschlüsselt, die den Einsatz einer PKI erfordern.

Im Folgenden soll der Verlauf einer Kommunikationsverbindung mit voriger Authentifizierung anhand der Abbildung 5 verdeutlicht werden.

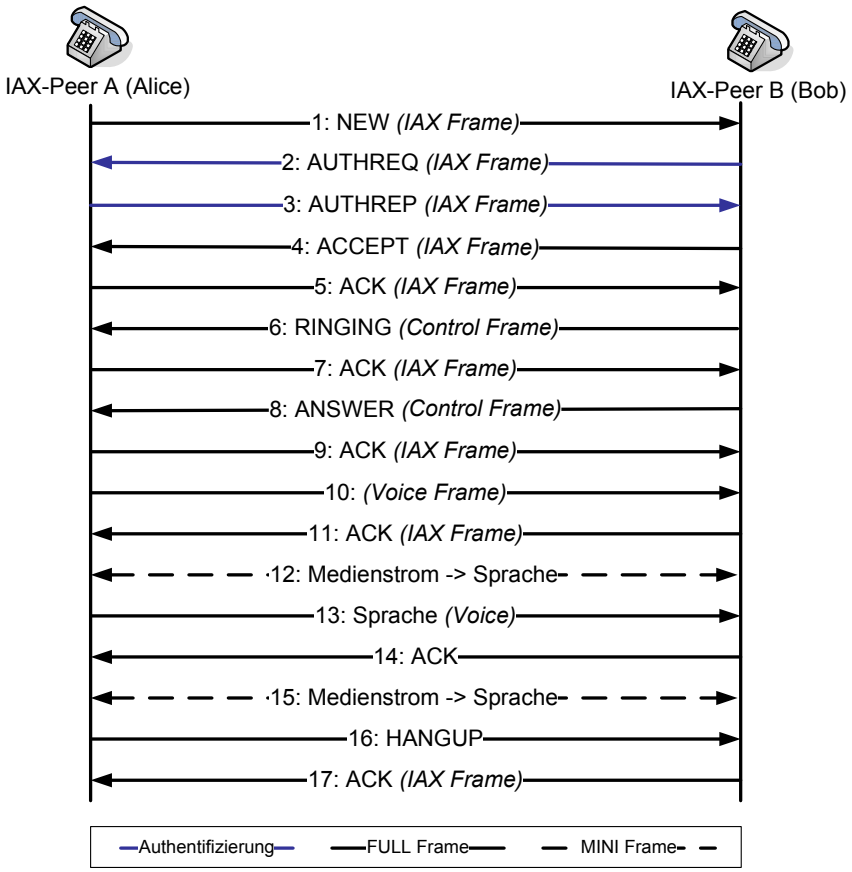

Abbildung 5: IAX Kommunikation

[60] Angenommen wird, dass die Netzwerkadresse des Kommunikationsteilnehmers nicht bekannt ist.

Die Anfrage einer Verbindung (*call leg*) wird vom *IAX-Peer* A (Alice) durch das Senden einer IAX-Nachricht mit dem Bezeichner *NEW* (*IAX-Event*) eingeleitet (1). Dabei besitzen alle IAX-Nachrichten innerhalb der Signalisierung den Pakettyp *Full-Frame*. In dieser Nachricht wird ebenfalls eine Liste mit Codecs übergeben, wobei die von Alice unterstützten gekennzeichnet sind.

Daraufhin fordert *IAX-Peer* B (Bob) durch Senden des IAX-Events *AUTHREQ* (2) eine vorherige Authentifizierung von Alice an. In dieser Nachricht werde die von ihm unterstützten Methoden zur Authentifizierung (MD-5, RSA) übergeben sowie einen Zufallswert (*Challenge*).

Alice berechnet daraufhin mit ihrem Passwort die *MD5-Challenge-Response* und sendet diese (*AUTHREP*) an Bob (3). Dieser bestätigt den erfolgreichen Aufbau der Verbindung mit dem IAX-Event *ACCEPT* (4) und übermittelt den für die Codierung der Sprachdaten verwendeten Codec, der wiederum von Alice durch ein *ACK* (5) bestätigt wird.

Bob signalisiert dem Anrufenden, dass er über den Wunsch des Verbindungsaufbaus informiert ist und sein Telefon klingelt. Dazu sendet er die Statusinformation (*Control-Frame*) *RINGING* (6), die von Alice wiederum durch das Senden eines *ACK* (7) bestätigt wird.

Wird die Verbindungsanfrage von Bob angenommen, schickt dieser das Control-Frame mit dem Bezeichner *ANSWER* (8), welches ebenfalls durch ein *ACK* (9) bestätigt wird. Daraufhin wird der Typ der Verbindung zwischen den beiden *Peers* verhandelt. Dazu sendet Alice eine Sprachnachricht (10) an Bob, in dieser der Verbindungstyp angegeben wird (*Voice*[61]). Dieser bestätigt den Erhalt der Nachricht durch ein *ACK* (11).

Daraufhin werden die Sprachdaten zwischen den beiden *Peers* unter Verwendung des Pakettyps *Mini-Frame* ausgetauscht (12). In regelmäßigen Abständen wird der Zustand der Sprachverbindung (12, 15) durch das Senden einer Sprachnachricht (13) und der entsprechenden Bestätigung (ACK) überprüft (14). Wird das Gespräch von Alice beendet, wird ein IAX-Event *HANGUP* (16) an Bob gesendet, der das Gesprächsende durch ein ACK (17) bestätigt.

Weiterhin wird die Verschlüsselung der Gesprächsdaten ebenfalls unter Verwendung des AES unterstützt[62]. Der Aufbau einer verschlüsselten Verbindung wird initiiert, indem im IAX-Event *NEW* der Parameter *ENCRYPTION* mit der Angabe der Verschlüsselungsmethode (AES-128) hinzugefügt wird. Aktuell wird ausschließlich der AES-Algorithmus mit 128 Bit Schlüssellänge unterstützt. Wenn der Angerufene ebenfalls diese Verschlüsselung unterstützt, sendet er eine Nachricht mit dem IAX-Event *AUTHREQ*, die ebenfalls den Parameter und die Methode zur Verschlüsselung enthält. Der Schlüssel zur Verschlüsselung wird erzeugt,

[61] Wahlweise sind auch Video, DTMF, Text oder auch HTML

[62] In Asterisk wird diese seit der Version 1.2.4 unterstützt und kann mit der Option *encryption=yes* und *encryption=aes128* in der *iax.conf* aktiviert werden.

indem der Zufallswert mit dem Passwort verknüpft wird und dann unter Verwendung des MD5-Algorithmus chiffriert wird. Mit dem Parameter *ENCKEY* wird zusätzlich die Möglichkeit gegeben, dass in einer bereits verschlüsselten Verbindung die Schlüssel für AES-Verschlüsselung gewechselt werden können.

2.2.8 IPSec

Internet Protocol Security (IPSec) wurde von der IETF zur Absicherung des Internetprotokolls [63] entwickelt. Dabei bietet IPSec durch den Einsatz des ESP-Protokolls im Tunnelmodus die Möglichkeit der Vernetzung zweier Standorte über ein nicht vertrauenswürdiges Netzwerk. Zudem kann durch die Verwendung des Internet Key Exchange (IKE)[64] das Schlüsselmaterial in Form von *Pre-Shared-Keys*, *Public-Keys* und Zertifikaten bereitgestellt werden [JP06; KA98a].

Das Encapsulated Security Payload (ESP) bietet Vertraulichkeit und Integrität für die übertragenen Daten, indem das gesamte IP-Paket in ein ESP-Paket gekapselt und um einen neuen IP-Header im Klartext erweitert wird. Durch eine angehängte Signatur (*ESP Auth*) wird das ESP-Paket vor Manipulation durch Dritte geschützt und durch die Verschlüsselung des gekapselten IP-Paketes die Vertraulichkeit der übertragenen Daten sichergestellt [KA98b].

Eine IPSec-konforme Umsetzung des Standards bietet das Projekt *FreeS/WAN* mit einer Software für Linuxsysteme. Nähere Informationen dazu sind in der Maßnahme M 5.83 „Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN“ der IT-Grundschutz-Kataloge zu finden [BSI05b, M 5.83, S. 2777 ff.].

Bezüglich der Umsetzung von IPSec in Verbindung mit VoIP nennt die BSI-Studie VoIPSEC jedoch einige Punkte, die bezüglich der Sprachqualität zu berücksichtigen sind [AAG+05, S. 117].

- Aufgrund der verschlüsselten TCP- und UDP-Header bei IPSec muss die bevorzugte Behandlung der VoIP-Pakete bei der Umsetzung von QoS-Maßnahmen aus dem IP-Header erkennbar sein.
- Die Notwendigkeit von 7 *Handshakes* beim Schlüsselaustausch (IKE) bei einer hergestellten Verbindung kann zu einer irritierenden Wartezeit führen.
- Durch die Nutzung des ESP im Tunnelmodus entstehen 44-48 zusätzliche Bytes *Overhead*, die zu berücksichtigen sind.
- Die Ver- und Entschlüsselung der Daten kann zur Erhöhung der Latenzzeit führen.

[63] IPv4 und IPv6
[64] [HC98]

2.2.9 Sicherer Schlüsselaustausch

Ein Problem beim Einsatz der IP-Telefonie ist der geeignete Austausch von Schlüsselmaterial. Die Ursache ist, dass SRTP von zahlreichen Herstellern von VoIP-Endgeräten (siehe Kapitel A.2) zur Absicherung der Sprachkommunikation eingesetzt wird, jedoch keinen Mechanismus zum Schlüsselaustausch bereitstellt. Somit ist durch die in diesem Kapitel beschriebenen Protokolle sicherzustellen, dass ein sicherer Austausch des Schlüsselmaterials erfolgt. Eine Übersicht über mögliche Verfahren und deren Eigenschaften gibt die Tabelle 3.

Schlüsselaustausch	erfordert PKI	Schlüsselerneuerung	Downgrade Schutz
SDES	nein	ja	nein
MIKEY-PSK	nein	ja	ja
MIKEY-PK	ja	ja	ja
MIKEY-DH	ja	ja	ja
MIKEY-DHHMAC	nein	ja	ja
ZRTP	nein	ja	ja

Tabelle 3: Verfahren zum Schlüsselmanagement [Win06]

ZRTP

Eine sichere Vereinbarung eines gemeinsamen Schlüssels innerhalb des RTP wird durch den Einsatz von ZRTP ermöglicht. Aufgrund der herstellerübergreifenden Nutzung von RTP zur Übertragung der Sprachdaten, erlaubt ZRTP die verschlüsselte Übertragung zwischen Kommunikationspartnern, die nicht das gleiche Signalisierungsprotokoll verwenden [JP06, S. 189]. Dazu wird das RTP um einen Bereich im *Header* erweitert, in dem die ZRTP-Nachrichten ausgetauscht werden. Die Vereinbarung des gemeinsamen Schlüssels erfolgt unter Verwendung des Diffie-Hellmmann-Verfahrens. Aus dem vereinbarten Schlüssel wird der *Master-Key* und -*Salt* für die Verschlüsselung mit dem SRTP berechnet. ZRTP stellt somit ein eigenständiges Protokoll da, für das der Einsatz einer PKI nicht notwendig ist [ZJC06].

Das Diffie-Hellman-Verfahren erfordert einen zusätzlichen Schutz gegenüber MitM-Angriffen[65], da sichergestellt werden muss, dass der Schlüsselaustausch auch authentifiziert erfolgte. ZRTP gewährleistet dies, indem von beiden Kommunikationspartnern ein *Hashwert*, im Folgenden Short Authentication String (SAS) genannt, gebildet wird, der bei einem Erstkontakt zu Beginn des Gesprächs auf Gleichheit überprüft werden muss. Sollten die beiden SAS nicht identisch sein, ist von einem MitM-Angriff auszugehen. Bei einem weiterem Gespräch ist eine

[65] Man-in-the-Middle (MitM)

erneute Überprüfung nicht notwendig, da der verifizierte SAS aus einem vorigen Gespräch in die Berechnung des aktuellen SAS mit einfließt. Ein Angreifer müsste somit in alle Gespräche bis hin zum ersten involviert gewesen sein. Weitere Parameter für die Berechnung des SAS sind, neben den SAS aus möglichen vorigen Gesprächen, die beiden über das Diffie-Hellman-Verfahren öffentlich ausgetauschten Schlüssel der Kommunikationspartner[66] [ZJC06].

ZRTP bietet mit dem bereitgestellten Verfahren und SRTP Vertraulichkeit für die Sprachübertragung, jedoch keine Authentifizierung. Um dies zu ermöglichen, muss ein gemeinsamer Schlüssel innerhalb der Signalisierung mit in die Berechnung des SAS-Wertes einfließen [JP06, S. 189].

MIKEY

Eine weitere Möglichkeit des Schlüsselmanagements für SRTP bietet Multimedia Internet KEYing (MIKEY). MIKEY ist ein Ende-zu-Ende Schlüsselaustauschprotokoll, das in RFC 3830[67] spezifiziert und speziell für die Bereitstellung von Schlüsselmaterial für Echtzeitanwendungen konzipiert ist. Ähnlich dem ZRTP arbeitet MIKEY dabei unabhängig von der eingesetzten Signalisierung und kann somit sowohl in SIP (SDP) als auch in H.323 (H.235.7) eingesetzt werden. Mögliche Einsatzszenarien für MIKEY sind *Unicast-* (*Peer-to-Peer*), *Multicast-* (*One-to-Many*) und Gruppen-Umgebungen (*Many-to-Many*) [ACL+04; IT05h].

MIKEY setzt die zwei verschiedenen Schlüsselarten TEK Generation Key (TGK) und Traffic-encrypting Key (TEK) ein. Bei der Anwendung von MIKEY in Verbindung mit SRTP ist der TEK dem vom SRTP bekannten *Master Key* gleich zu setzen. Das bedeutet, dass die vom TGK abgeleiteten Schlüssel (TEK) direkt zur Verschlüsselung bei SRTP verwendet werden [JP06, S. 176].

Im RFC 3830 werden drei Modi[68] für den Schlüsselaustausch definiert. Der Austausch kann über *Pre-Shared Keys* (PSK), *Public Keys* (PK) und die Möglichkeit des Diffie-Hellman-Verfahrens[69] erfolgen. Beim Einsatz der PSK ist keine PKI notwendig, da davon ausgegangen wird, dass die Gesprächsteilnehmer bereits vorab einen Schlüssel ausgetauscht haben. Bei der Verwendung der PK ist eine PKI notwendig, damit den Gesprächsteilnehmern die öffentlichen Schlüssel der Gesprächspartner sicher zur Verfügung gestellt werden können. Beide Mechanismen haben gemeinsam, dass ein oder mehrere TGK und zusätzliche Sicherheitsparameter sicher an den oder die Gesprächsempfänger übertragen werden. Hingegen wird beim Einsatz des Diffie-Hellmann-Verfahrens der TGK von den Gesprächsteilnehmern durch die ausgetauschten Parameter eigenständig generiert [ACL+04, Kap. 3].

[66] sasvalue = hash(pvi | pvr | „Short Authentication String“) [ZJC06, Kap. 6]
[67] [ACL+04]
[68] MIKEY-PSK, MIKEY-PK und MIKEY-DH
[69] Die Implementierung von DH ist in [ACL+04] als optional gekennzeichnet und nur für die Vereinbarung von Schlüssel in Unicast-Verbindungen geeignet.

Zusätzlich wird im RFC 4650[70] ein Modus definiert, welcher die Modi *MIKEY-DH* und *MIKEY-PSK* vereint, indem ein sogenannter *keyed HMAC*[71] zur Sicherstellung der Authentizität des ausgetauschten Diffie-Hellmann-Parameters eingesetzt wird. Eine Übersicht über aktuelle MIKEY-Modi bieten die Dokumente [FI06] und [Win06].

Ähnlich wie die bei H.235 verwendeten Sicherheitsprofile, müssen die bei MIKEY eingesetzten Modi von allen beteiligten Kommunikationspartnern unterstützt werden. Somit ist zu Beginn ein von allen Teilnehmern unterstützter Modus zu vereinbaren [JP06, S. 173].

SDES und TLS

Eine weitere Möglichkeit der Bereitstellung des Schlüsselmaterials für das SRTP stellt die Verwendung des SDP dar. Dabei wird im RFC 4568[72] ein zusätzliches Attribut *crypto* zur Übertragung der zum Schlüsselmanagement erforderlichen Parameter definiert. Dazu gehören Verschlüsselungs- und Signaturalgorithmen (AES_CM_128 und HMAC_SHA1_80), das Schlüsselmaterial (inline:[xxx]) und dessen Gültigkeitsdauer für RTP-Pakete (2^{20}) sowie sein Indikator und seine Länge in Bits (1:32). Der Einsatz des Attributes *crypto* ist jedoch auf die Übertragung von *Unicast-Verbindungen* zwischen zwei Kommunikationspartnern beschränkt.

```
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32
```

Die Übertragung der Parameter erfolgt innerhalb des SDP im Klartext. Somit erfordert diese Möglichkeit, auch Security Descriptions (SDES) genannt, dass zusätzlich die Signalisierung und somit die Übertragung des Schlüssels verschlüsselt erfolgt. Bei Implementierungen des SIP wird die Verwendung von SDES in Verbindung mit TLS[73] am häufigsten von den Herstellern realisiert.

[70] [Euc06]
[71] Hash Message Authentication Code (HMAC)
[72] [ABW06]
[73] Da TLS auf dem TCP aufbaut, müssen die Geräte gegenüber dem herkömmlichen UDP zusätzlich das TCP unterstützen.

3 Prüfschema

3.1 Methodik

In der Methodik werden etablierte Verfahren der IT-Grundschutz-Vorgehensweise [BSI05a] aufgegriffen. Dabei handelt es sich um die Modellierung eines IT-Verbundes durch Bausteine und einen Soll-Ist-Vergleich von Maßnahmen. Grundlage für die Methodik sind, analog zu den IT-Grundschutzkatalogen, ein Gefährdungskatalog und ein Maßnahmenkatalog. Um ein Auditieren der VoIP-Infrastrukturen zu vereinfachen, wird im Vergleich zu der IT-Grundschutz-Vorgehensweise die Methodik um Prüfkriterien erweitert.

Zunächst soll die VoIP-Infrastruktur durch die im Kapitel 3.2 beschriebenen Module abgebildet werden (Modellierung). Dadurch können für diese Infrastruktur Angaben bezüglich der Gefährdungslage und der durchzuführenden Maßnahmen gemacht werden. Dieses Kapitel stellt somit den Ausgangspunkt für eine Bewertung der Sicherheitsdefizite dar (siehe Abbildung 6).

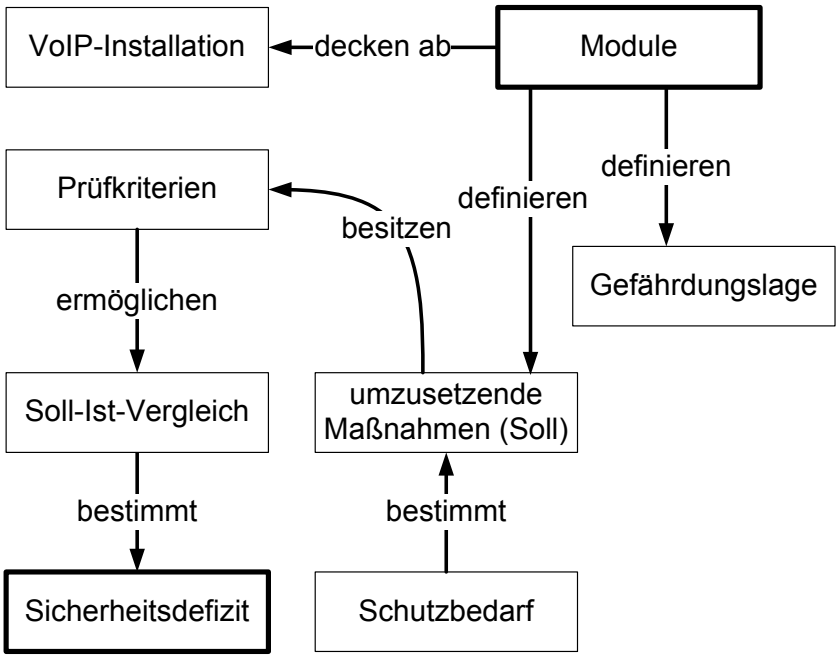

Abbildung 6: Prüfschema

In jedem Modul wird, ähnlich den Bausteinen der IT-Grundschutz-Kataloge, ein Überblick über die Gefährdungslage der individuellen Komponente gegeben. Dies erfolgt in dieser Arbeit durch eine Gefährdungsübersicht in Form einer Tabelle. Eine genaue Beschreibung der jeweiligen Gefährdungen erfolgt im Kapitel 4.2,

in dem alle zu betrachtenden Gefährdungen, ähnlich dem Gefährdungskatalog der IT-Grundschutz-Kataloge, zusammengefasst werden. Die dokumentierten Gefährdungen beziehen sich in dieser Arbeit ausschließlich auf VoIP-Infrastrukturen. Um einen netzwerkweiten Grundschutz zu etablieren, sind zusätzlich die zutreffenden Bausteine der IT-Grundschutz-Kataloge anzuwenden.

Neben einer Gefährdungsübersicht werden Maßnahmen beschrieben, die für dieses Modul abhängig vom jeweiligen Schutzbedarf umzusetzen sind (siehe Kapitel 5.2). Dies setzt eine Schutzbedarfsfeststellung nach IT-Grundschutz-Vorgehensweise voraus. „*Ziel der Schutzbedarfsfeststellung ist es, ausgehend von den Geschäftsprozessen für jede erfasste IT-Anwendung einschließlich ihrer Daten zu entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzt. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen IT-Anwendung und damit der jeweiligen Geschäftsprozesse verbunden sind.*“ [BSI05a, S. 41] Die Module stellen somit sicher, dass die Maßnahmen abhängig vom Geschäftsrisiko umgesetzt und für jede Gefährdung eines Moduls etablierte Verfahren zur Absicherung eingesetzt werden.

Mögliche Kategorien für den Schutzbedarf sind normal und hoch. Dabei müssen Maßnahmen der Kategorie normal verpflichtend umgesetzt werden. Maßnahmen der Kategorie hoch sind dann umzusetzen, wenn erhöhte Anforderungen beispielsweise an die Verfügbarkeit des Telefoniedienstes gestellt werden. Darüber hinaus können Zusatzmaßnahmen getroffen werden, die einen erhöhten Schutz gegenüber Angriffen bieten oder bei auftretenden Störungen durch Werbeanrufe diese unterbinden können.

Die in Kapitel 6.2 beschrieben Prüfkriterien ermöglichen es, die Umsetzung der Maßnahmen in einem Soll-Ist-Vergleich zu überprüfen. Die Anforderungen der Prüfkriterien können anhand von Datenblättern, Interviews, den Konfigurationseinstellungen und durch den Einsatz von Audit-Tools (siehe A.1) geprüft werden. Das Ergebnis dieses Soll-Ist-Vergleiches zeigt die Sicherheitsdefizite der VoIP-Infrastruktur auf und bildet die Grundlage für die Umsetzung der defizitären Maßnahmen.

3.2 Module

3.2.1 IP-Telefonanlage

Charakteristisch für eine IP-Telefonanlage *(IP-PBX)* gegenüber einer ISDN-TK-Anlage ist, dass die Übertragung der digitalisierten Sprache über paketorientierte Netze erfolgt und sie somit in eine bestehende IP-Infrastruktur integriert werden kann. Wie leitungsvermittelnde TK-Anlagen übernimmt die IP-PBX die Anrufverarbeitung und Vermittlungsfunktionen für interne als auch externe Telefongespräche. Bei der Vermittlung von Gesprächen zu externen Kommunikationspartnern erfolgt die Übertragung der Signalisierung und der Sprachdaten, abhängig von der Außenanbindung, über öffentliche IP-Netze oder das Fernsprechnetz (siehe Modul IP-Gateway und ISDN-Gateway). Ferner übernimmt die IP-PBX auch die Authentifizierung und Registrierung der Teilnehmer und integriert damit, abhängig vom VoIP-Protokoll (siehe Kapitel 2.2), die Funktion eines Proxies (Registrars), Gatekeepers oder Call-Managers.

Im Netzwerkverbund ist eine IP-PBX als zusätzlicher Server zu verstehen, der mit einem weiteren Dienst die Übertragung eines neuen Mediums (Sprache) im Netzwerk ermöglicht. Die Integration der Sprache birgt jedoch zusätzliche Gefahren, die durch geeignete Maßnahmen beseitigt werden müssen. Die Gefährdungslage und die umzusetzenden Sicherheitsmaßnahmen beim Einsatz einer IP-PBX sollen im Folgenden aufgezeigt werden.

Gefährdungslage

Beim Einsatz einer IP-Telefonanlage werden die folgenden Gefährdungen angenommen.

Gefährdungen
G 1 Abhören von Gesprächen
G 3 Bekanntwerden von Kommunikationsprofilen
G 4 Unbefugter Zugriff auf Konfigurationseinstellungen
G 5 Ausnutzen von Implementierungsfehlern
G 6 Bekanntwerden interner vertraulicher Informationen
G 7 Gebührenbetrug
G 8 Kompromittierung von Registrierungsinformationen
G 9 Vortäuschung einer Identität
G 10 Verlust und Beeinträchtigung der Verfügbarkeit
G 11 Manipulation von Sprachdaten
G 12 Abstreitbarkeit von Gesprächen
G 13 Unbefugter Zutritt zu Basiskomponenten
G 16 Kopplung von Ausfallrisiken

Tabelle 4: Gefährdungen beim Einsatz von IP-Telefonanlagen

Sicherheitsmaßnahmen

Für den sicheren Einsatz einer IP-Telefonanlage *(IP-PBX)* müssen abhängig vom Schutzbedarf die im Folgenden beschriebenen Maßnahmen umgesetzt werden. Eine Übersicht über die Maßnahmen und deren Schutzbedarfskategorie liefert die Tabelle 5 zum Ende des Kapitels.

VoIP-spezifische Maßnahmen

Werden im Netzwerk CoS-Mechanismen[74] zum Bandbreitenmanagement eingesetzt, muss die IP-PBX die Markierung von Sprachpaketen unterstützen (M 5). Dies ist notwendig, da die Daten an Knotenpunkten wie Routern und Switches nur bevorzugt behandelt werden können, wenn sie durch den Sender entsprechend klassifiziert wurden.

Beim Einsatz einer IP-PBX ist eine verschlüsselte Übertragung der Signalisierungs- und Sprachdaten (siehe M 7 und M 8) umzusetzen. Diese verhindert zum einen, dass Daten von Dritten manipuliert werden. Andererseits wird sichergestellt, dass vertrauliche Informationen wie Gesprächsinhalte nicht abgehört werden können. Die zur Verschlüsselung eingesetzten Protokolle müssen von der IP-PBX als auch von den IP-Telefonen umgesetzt werden, um wirksam zu sein. Beim Einsatz des SRTP (siehe Kapitel 2.2.5) zur Verschlüsselung der Sprachdaten muss durch die in Kapitel 2.2.9 beschrieben Protokolle der sichere Austausch des Schlüsselmaterials gewährleistet sein.

Abhängig vom Einsatzzweck eines IP-Telefons sind die Wahlmöglichkeiten und die verfügbaren Leistungsmerkmale für den Nutzer durch eine Zuordnung von Profilen (siehe M 12) anzupassen. Diese müssen auf öffentlich zugängliche IP-Telefone angewandt werden, um einen Gebührenbetrug auszuschließen. Auch die Anwendung auf alle IP-Telefone reduziert zusätzliche Kosten, welche durch einige Leistungsmerkmale oder teure Servicenummern verursacht werden können.

Eine Authentifizierung der Endgeräte (siehe M 14) gegenüber der IP-PBX ist ebenso notwendig, um zusätzliche Kosten durch Gebührenbetrug zu vermeiden oder die Möglichkeit der Gebührenaufschlüsselung zu haben. Die Verfahren zur Authentifizierung müssen zusätzlich die Integrität der übertragenen Daten sicherstellen. Für eine starke Authentifizierung ist der Identitätsnachweis durch Zertifikate umzusetzen.

Um die Angriffsmöglichkeiten beim Einsatz einer IP-PBX einzuschränken, muss diese systemspezifisch *gehärtet* werden. Das bedeutet unter anderem, dass kritische Leistungsmerkmale deaktiviert werden und nur notwendige Dienste aktiv sind. Weitere Kriterien zur *Härtung* der IP-PBX können der Maßnahme M 17 „Absichern der IP-Telefonanlage“ entnommen werden. Der Umfang der Absicherung kann abhängig von der eingesetzten Lösung unterschiedlich ausfallen. So

[74] Class of Service (CoS)

besitzen bestimmte IP-PBX bereits gehärtete und auf die Funktionalität des Systems zugeschnittene Betriebssysteme. Der Einsatz dieser proprietären Lösungen bedeutet auch, dass sich nicht immer alle Kriterien umsetzen lassen, wenn nur vordefinierte Einstellungen über eine Management-Oberfläche vorgenommen werden können. Andererseits müssen beim Einsatz von Betriebssystemen, wie Linux und Windows, zusätzliche Kriterien zur Absicherung herangezogen werden.

Sicherer Betrieb

Für den sicheren Betrieb einer IP-PBX muss gewährleistet werden, dass sicherheits- und systemkritische Ereignisse zentral protokolliert und ausgewertet werden. Um den Aufwand der Auswertung gering zu halten, sollte diese durch spezielle Tools erfolgen, die zusätzlich bei Auffälligkeiten eine Benachrichtigung ermöglichen. Kriterien für die Protokollierung sind der Maßnahme M 6 „Monitoring und Logging“ zu entnehmen.

Bei der IP-PBX müssen die Remote-Schnittstellen gegenüber unbefugten Dritten abgesichert werden (siehe M 9), um eine unberechtigte Verwaltung der IP-Telefonanlage auszuschließen und den Zugriff auf sicherheitskritische Informationen zu unterbinden. Remote-Schnittstellen, die nicht verwendet werden, müssen deaktiviert werden, um die Anforderung der minimalen Dienste[75] zu erfüllen.

Für den sicheren Betrieb sind abschließend Angriffe auf die Basis-Netzwerkdienste (DHCP[76] und ARP[77]) gemäß der in Maßnahme M 18 beschriebenen Möglichkeiten abzusichern. Das bedeutet für die Umsetzung, dass gängige Angriffe auf die IP-Telefonanlage von ihr erkannt werden oder zusätzliche Maßnahmen ergriffen werden müssen, die diese Funktion für das Netzwerk oder ein Netzsegment übernehmen (siehe Maßnahme M 23 „Einsatz von IDS“ oder die Umsetzung von M 18 in dem Modul Switches und Router).

Planung und Konzeption

Um die Verfügbarkeit des Telefoniedienstes im Rahmen eines Redudanzkonzeptes zu steigern, muss eine IP-Telefonanlage ebenfalls berücksichtigt werden (siehe M 1).

Für eine IP-PBX ist ebenso wie für andere Netzkomponenten sicherzustellen, dass mögliche Sicherheitslücken durch Patches zeitnah beseitigt werden oder Maßnahmen zur Absicherung ergriffen werden. Weitere Anforderungen an das umzusetzende Patchmanagement sind in Maßnahme M 13 genannt.

Die IP-PBX muss weiterhin vor dem physikalischen Zugriff durch unbefugte Dritte geschützt werden, indem sie in gesicherten Räumlichkeiten untergebracht ist. Dort sollte sie ebenfalls vor kurzzeitigen Stromausfällen durch eine USV-Anlage[78]

[75] siehe Maßnahme M 17 „Absichern der IP-Telefonanlage“
[76] Dynamic Host Configuration Protocol (DHCP)
[77] Address Resolution Protocol (ARP)
[78] Unterbrechungsfreie Stromversorgung (USV)

geschützt werden. Nähere Angaben sind den Maßnahmen M 19 „USV für die Middleware“ und M 21 „Physische Zutrittskontrolle“ zu entnehmen.

Maßnahmen	Schutzbedarf	
	normal	hoch
M 1 Redundante Auslegung wichtiger Netzkomponenten		X
M 5 Bandbreitenmanagement	X	X
M 6 Monitoring und Logging	X	X
M 7 Verschlüsselung der Signalisierung	X	X
M 8 Verschlüsselung der Sprachdaten	X	X
M 9 Absichern der Remote-Schnittstellen	X	X
M 12 Einsatz von Profilen für Endgeräte	X	X
M 13 Patchmanagement	X	X
M 14 Authentifizierung der Endgeräte	X	X
M 17 Absichern der IP-Telefonanlage	X	X
M 18 Absichern der Basis-Netzwerkdienste		X
M 19 USV für die Middleware		X
M 21 Physische Zutrittskontrolle	X	X
M 23 Einsatz von IDS	ZM	ZM

Tabelle 5: Maßnahmen beim Einsatz von IP-Telefonanlagen (ZM = Zusatzmaßnahme)

3.2.2 ISDN-Gateway

Ein ISDN-Gateway (VoIP-Gateway) bietet eine Schnittstelle zwischen analogen beziehungsweise digitalen Fernsprechnetzen (PSTN) und IP-Netzwerken. Damit wird die Vermittlung zwischen paketorientierten und leitungsvermittelnden Netzen ermöglicht. Um diese netzübergreifenden Gespräche zu bewerkstelligen, muss das ISDN-Gateway zwischen dem kontinuierlichen Bitstrom (64kbit/s) des Fernsprechnetzes und den Paketen des IP-Netzwerkes konvertieren.

Durch den Einsatz eines ISDN-Gateways ist eine nahtlose Migration von der klassischen TK-Infrastruktur zu einer reinen VoIP-Infrastruktur möglich. Dabei entstehen sogenannte Insellösungen. Das bedeutet, dass Firmen im Local Area Network (LAN) bereits auf VoIP umgestellt haben, jedoch die Gespräche weiterhin über den Telefonanschluss in das Fernsprechnetz vermittelt werden. Diese Außenanbindung hat den Vorteil, dass mögliche Angriffsszenarien von extern sich

lediglich auf das Fernsprechnetz beschränken und somit weniger Gefahrenquellen, gegenüber einer Außenanbindung über ein öffentliches IP-Netz, existieren.

Zusätzlich bietet ein ISDN-Gateway die Möglichkeit, die Notruf-Funktionalität sicherzustellen. Dies ist ein entscheidender Vorteil aufgrund der unzureichend umgesetzten Notrufanforderungen bei VoIP (siehe Gefährdung G 15). Für das Modul ISDN-Gateway ist neben dem Modul IP-Telefonanlage (siehe Kapitel 3.2.1) zusätzlich der Baustein B 3.401 „TK-Anlage“ der IT-Grundschutz-Kataloge anzuwenden [BSI05b, S.190 ff.].

Gefährdungslage und Maßnahmenempfehlung

Für ein ISDN-Gateway gelten aufgrund seiner Funktion als Vermittler sowohl die Gefährdungen einer TK-Anlage (siehe [BSI05b, S. 190 ff.]) als auch die einer IP-Telefonanlage (siehe Tabelle 4). Dementsprechend sind die zugehörigen Maßnahmen ebenso auf ein ISDN-Gateway anzuwenden (siehe [BSI05b, S. 191 ff.] und Tabelle 5).

3.2.3 IP-Gateway

Ein IP-Gateway ist eine zusätzliche Komponente für eine IP-PBX, welche die Anbindung an ein öffentliches VoIP-Netzwerk (WAN) ermöglicht. Somit kann abhängig vom Kommunikationspartner, die Übertragung der Sprachverbindungen ausschließlich über IP-basierte Netzwerke erfolgen. Dies birgt neben zusätzlichen Gefahren, die aus der öffentlichen IP-Anbindung resultieren, auch die Möglichkeit der kostengünstigen Anbindung von Standorten. Der Grund für die geringeren Kosten ist, dass eine bestehende Internetanbindung verwendet werden kann und so keine zusätzlichen Kosten für die Vermittlung in öffentliche Fernsprechnetze entstehen. Es ist jedoch zusätzlich zu prüfen, ob die bestehende Internetanbindung für die zusätzliche Übertragung der Sprachdaten ausreichend dimensioniert ist. Bis auf einige Ausnahmen bestehen für das IP-Gateway aufgrund der engen Verzahnung mit der IP-Telefonanlage die gleichen Gefährdungen und umzusetzenden Maßnahmen. Die Unterschiede sollen im Folgenden beschrieben werden.

Gefährdungslage

Beim Einsatz einer IP-Telefonanlage mit einem zugehörigen IP-Gateway sollten die folgenden Gefährdungen zusätzlich berücksichtigt werden.

Gefährdungen
G 14 Unerwünschte Werbeanrufe
G 15 Fehlende oder eingeschränkte Notrufmöglichkeit

Tabelle 6: Gefährdungen beim Einsatz von IP-Gateways

Maßnahmenempfehlung

Bei einer externen IP-Anbindung muss die lokale Infrastruktur durch eine Firewall oder einen Session Border Controller (SBC) gegenüber Angriffen aus dem öffentlichen VoIP-Netzwerk geschützt werden. Ferner muss bei Netzübergängen zu externen VoIP-Netzwerken die Firewall- und NAT-Problematik berücksichtigt werden (M 16).

Beim Einsatz von IP-Gateways ist weiterhin zu beachten, dass die Notrufmöglichkeit bei VoIP bisher unzureichend umgesetzt ist und somit durch zusätzliche Maßnahmen sicherzustellen ist. Möglichkeiten, den Notrufanforderungen gerecht zu werden, sind in der Maßnahme M 22 „Sicherstellen der Notrufmöglichkeit“ genannt. Sollten vermehrt unerwünschte Werbeanrufe auftreten, kann die Maßnahme M 24 hinzugezogen werden.

Maßnahmen	Schutzbedarf	
	normal	hoch
M 16 Absicherung der Netzübergänge zu öffentlichen VoIP-Netzwerken	X	X
M 22 Sicherstellen der Notrufmöglichkeit	X	X
M 24 Maßnahmen gegen automatisierte unerwünschte Werbeanrufe	ZM	ZM

Tabelle 7: Maßnahmen beim Einsatz von IP-Gateways (ZM = Zusatzmaßnahme)

3.2.4 IP-Telefon

Ein IP-Telefon wird über ein lokales IP-basiertes Netzwerk (LAN) mit der IP-Telefonanlage verbunden. Eine Anbindung der Telefone über ein bisher verwendetes Telefonnetz entfällt somit. Mit dem IP-Telefon kann ein im Netzwerk angebotener Telefoniedienst unabhängig vom aktuellen Standort genutzt werden. Mit den in diesem Kapitel beschriebenen Modulen lassen sich sowohl interne als auch externe Gespräche mit den gleichen Merkmalen und in gewohnter Qualität führen.

Die Konfiguration der IP-Telefone für das LAN erfolgt unter Verwendung des DHCP. Die Einrichtung kann am Gerät selbst oder über Remote-Schnittstellen vorgenommen werden. In großen Netzwerkumgebungen wird die Konfiguration zahlreicher IP-Telefone durch die Bereitstellung zentraler Konfigurationsdateien ermöglicht. Zusätzlich kann Power over Ethernet (PoE) die Stromversorgung der IP-Telefone über das Netzwerk übernehmen, so dass Netzteile für die Endgeräte nicht benötigt werden.

IP-Telefone unterscheiden sich im Allgemeinen grundlegend durch das verwendete Signalisierungsprotokoll und somit durch protokollspezifisch umgesetzte Leistungsmerkmale. Gängige Signalisierungsprotokolle sind im Kapitel 2.2 Protokolle besprochen worden.

Gefährdungslage

Beim Einsatz von IP-Telefonen liegen die folgenden Gefährdungen vor.

Gefährdungen
G 1 Abhören von Gesprächen
G 2 Abhören von Räumen mit Endgeräten
G 3 Bekanntwerden von Kommunikationsprofilen
G 4 Unbefugter Zugriff auf Konfigurationseinstellungen
G 5 Ausnutzen von Implementierungsfehlern
G 6 Bekanntwerden interner vertraulicher Informationen
G 7 Gebührenbetrug
G 8 Kompromittierung von Registrierungsinformationen
G 9 Vortäuschung einer Identität
G 10 Verlust und Beeinträchtigung der Verfügbarkeit
G 11 Manipulation von Sprachdaten
G 12 Abstreitbarkeit von Gesprächen

Tabelle 8: Gefährdungen beim Einsatz von IP-Telefonen

Maßnahmenempfehlung

Für den sicheren Einsatz von IP-Telefonen müssen abhängig vom Schutzbedarf die im Folgenden beschriebenen Maßnahmen umgesetzt werden. Eine Übersicht über die Maßnahmen und deren Schutzbedarfskategorie liefert die Tabelle 9 zum Ende des Kapitels.

VoIP-spezifische Maßnahmen

Bei der Übertragung der Signalisierungs- und Sprachdaten muss sichergestellt werden, dass die Dienstgüte der Sprachverbindung den Anforderungen entspricht. Kommen beim Bandbreitenmanagement CoS-Mechanismen zum Einsatz, müssen die Endgeräte die Markierung von IP-Paketen (*DiffServ*) beziehungsweise *Ethernet-Frames* (802.1Q/p) unterstützen. Dies ermöglicht, dass Sprachpakete an Netzknoten wie Switches und Routern bevorzugt behandelt werden können. Detaillierte Informationen bezüglich der Maßnahmen zum Bandbreitenmanagement sind in Maßnahme M 5 dokumentiert.

Um die Integrität und Vertraulichkeit der übertragenen Sprache sicherzustellen, sind die Sprachdaten verschlüsselt zu übertragen (M 8). Dies erfordert zusätzlich den sicheren Austausch von Schlüsselmaterial, welcher durch den Einsatz von

Schlüsselmanagementprotokollen (siehe Kapitel 2.2.9) gewährleistet werden kann oder durch einen Austausch innerhalb der verschlüsselten Signalisierung (M 7). Ein verschlüsselter Transport der Signalisierungsdaten stellt zudem sicher, dass keine Kommunikationsprofile anhand der Signalisierung erstellt und Gefahren durch die Manipulation der Signalisierungsdaten ausgeschlossen werden können.

Einige IP-Telefone ermöglichen mit Hilfe eines Multiports den Anschluss eines Computers und eines IP-Telefons über ein Netzwerkkabel. Somit lassen sich die notwendigen Netzwerkanschlüsse und Kabel im Netzwerk reduzieren. Allerdings werden dadurch IP-Telefon und Computer im gleichen Netzsegment betrieben, was der in Maßnahme M 2 beschriebenen Trennung von Sprach- und Datennetz widerspricht. Für den sicheren Betrieb des Multiports ist die Maßnahme M 10 „Absichern der Multiportfunktion“ umzusetzen.

Durch den Einsatz im Netzwerk und die integrierte Funktionalität bieten IP-Telefone ähnliche Angriffsmöglichkeiten wie Computer und müssen vor dem Einsatz sicher konfiguriert werden (M 11).

Zur sicheren Authentifizierung der Endgeräte sollte mindestens ein *Challenge-Response-Verfahren* eingesetzt werden. Dieses ermöglicht die sichere Übertragung der Authentifizierungsdaten zur IP-Telefonanlage, ohne dass Passwörter im Klartext übertragen werden. Somit kann sichergestellt werden, dass Angreifer, die Zugang zum Netz besitzen, die Daten nicht mitlesen und für einen Gebührenbetrug einsetzen können. Zusätzlich sollten allerdings alle Passwörter bezüglich der Komplexität ausreichend sicher gewählt werden. Weitere Kriterien und Verfahren zur Authentifizierung sind der Maßnahme M 14 „Authentifizierung der Endgeräte“ zu entnehmen.

Sicherer Betrieb

IP-Telefone müssen ähnlich der IP-Telefonanlage in einen netzwerkweiten Monitoring- und Logging-Dienst integriert werden (M 6). Abhängig vom Umfang der protokollierten Ereignisse besteht die Möglichkeit der einfachen Diagnose einer Fehlkonfiguration und einen Überblick über den Zustand des Gerätes zu erhalten. Wenn eine Gebührenaufschlüsselung umgesetzt werden soll, können die notwendigen Informationen wie Dauer und Rufnummer des Gesprächs ebenfalls durch die Protokollierung der IP-Telefone gespeichert werden.

Für den sicheren Betrieb der IP-Telefone müssen die Remote-Schnittstellen wirksam abgesichert werden (M 9). Da ein unbefugter Zugriff aufgrund der zahlreichen Folgegefährdungen ein hohes Risiko darstellt (Gefährdung G 4). Werden die IP-Telefone nicht über die Remote-Schnittstelle administriert, ist diese zu deaktivieren.

Wird im Netzwerk eine Endgeräteauthentifizierung nach dem IEEE-Standard 802.1X umgesetzt, müssen die IP-Telefone diese ebenfalls unterstützen. Anforderungen zur portbasierten Authentifizierung bei IP-Telefonen sind in der Maßnahme M 15 „Sichere Endgeräteauthentifizierung mittels IEEE 802.1X“ dokumentiert.

Planung und Konzeption

Durch mögliche Schwachstellen bei der Verarbeitung von VoIP-Protokollen ist es notwendig, dass IP-Telefone in das Patchmanagement einbezogen werden (M 13). Dies soll sicherstellen, dass veröffentlichte Patches zeitnah eingespielt werden. Zusätzlich müssen veröffentlichte Sicherheitslücken den Betreibern bekannt sein, um gegebenenfalls vor der Veröffentlichung des Patches Maßnahmen für den sicheren Betrieb umzusetzen.

Bei hohem Schutzbedarf ist ebenfalls die unterbrechungsfreie Stromversorgung für IP-Telefone nach Maßnahme M 20 „USV für IP-Telefone“ sicherzustellen. Dies erfordert, dass von den Switches und IP-Telefonen eine Stromversorgung durch PoE unterstützt wird.

Maßnahmen	Schutzbedarf	
	normal	hoch
M 5 Bandbreitenmanagement	X	X
M 6 Monitoring und Logging	X	X
M 7 Verschlüsselung der Signalisierung	X	X
M 8 Verschlüsselung der Sprachdaten	X	X
M 9 Absichern der Remote-Schnittstellen	X	X
M 10 Absichern der Multiportfunktion	X	X
M 11 Sichere Konfiguration der IP-Telefone	X	X
M 13 Patchmanagement	X	X
M 14 Authentifizierung der Endgeräte	X	X
M 15 Sichere Endgeräteauthentifizierung mittels IEEE 802.1X		X
M 20 USV für IP-Telefone		X

Tabelle 9: Maßnahmen beim Einsatz von IP-Telefonen

3.2.5 Switches und Router

Switches bieten in VoIP-Netzwerken die Möglichkeit, angeschlossene Endgeräte auf Schicht 2 des ISO/OSI-Referenzmodells zu vernetzen. Router dagegen arbeiten auf ISO/OSI-Schicht 3 und ermöglichen die Weiterleitung von IP-Paketen zwischen unterschiedlichen Subnetzen. Beide Komponenten spielen daher eine zentrale Rolle bei der Kommunikation zwischen einzelnen VoIP-Komponenten. Welche Möglichkeiten deren Einsatz bietet und welche Auswirkungen dies auf die Sicherheit eines VoIP-Netzwerkes haben kann, soll in den folgenden Abschnitten beschrieben werden.

Gefährdungslage

Beim Einsatz von Switches und Routern werden die folgenden Gefährdungen angenommen.

Gefährdungen
G 1 Abhören von Gesprächen
G 4 Unbefugter Zugriff auf Konfigurationseinstellungen
G 5 Ausnutzen von Implementierungsfehlern
G 6 Bekanntwerden interner vertraulicher Informationen
G 8 Kompromittierung von Registrierungsinformationen
G 10 Verlust und Beeinträchtigung der Verfügbarkeit
G 13 Unbefugter Zutritt zu Basiskomponenten
G 16 Kopplung von Ausfallrisiken

Tabelle 10: Gefährdungen beim Einsatz von Switches und Routern

Maßnahmenempfehlung

Für den sicheren Einsatz von Switches und Routern müssen abhängig vom Schutzbedarf die im Folgenden beschriebenen Maßnahmen umgesetzt werden. Eine Übersicht über die Maßnahmen und deren Schutzbedarfskategorie liefert die Tabelle 11 zum Ende des Kapitels.

VoIP-spezifische Maßnahmen

Neben der Vernetzung einzelner Komponenten und der Zusammenführung von Netzsegmenten haben Switches und Router in einem VoIP-Netzwerk zusätzlich die Aufgabe, das Sprach- und Datennetz zu trennen (M 2). Für den Endgerätezugang kann eine Trennung durch die logische oder physikalische Segmentierung umgesetzt werden. Ferner müssen für Sprach- und Datennetz unterschiedliche private Adressbereiche definiert werden.

Wird das Bandbreitenmanagement (siehe Maßnahme M 5) durch eine Überdimensionierung der Bandbreite umgesetzt (Overprovisioning), muss die Link-Datenrate der Switches und Router den Anforderungen entsprechend ausgelegt

sein. Kommen CoS- oder QoS-Mechanismen zum Einsatz, muss sichergestellt sein, dass diese von den Switches und Routern unterstützt werden. Dies ist notwendig, um die Priorisierung der Sprachpakete auswerten zu können und die Pakete beim Transport entsprechend ihrer Klassifizierung weiterzuleiten.

Sicherer Betrieb

Die Protokollierung (M 6) bei Switches und Routern stellt ebenfalls eine Notwendigkeit dar, um bei Angriffen, Änderungen an der Konfiguration, Statusmeldungen und vergleichbaren Ereignissen die Möglichkeit der Auswertung und Analyse zu besitzen.

Für den sicheren Betrieb von Switches und Routern sind nach M 9 die Remote-Schnittstellen abzusichern, um Angreifer keine Möglichkeit zu geben, Zugriff auf die Konfiguration zu erhalten.

Um den Zugang zum Netzwerk bei hohem Schutzbedarf wirkungsvoll einzuschränken, müssen Switches und Router die Endgeräteauthentifizierung nach dem IEEE-Standard 802.1X umsetzen (M 15). Zusätzlich ist es erforderlich, dass alle Endgeräte eine portbasierte Zugangskontrolle nach IEEE 802.1X unterstützen und ein zentraler Authentifizierungsserver zur Verfügung steht.

Für den sicheren Betrieb eines VoIP-Netzwerkes erkennen einige Switches und Router Angriffe auf Protokolle wie das ARP und das DHCP und können den Versand von manipulierten Paketen unterbinden. Somit ist ein Absicherung der Basis-Netzwerkdienste nach Maßnahme M 18 möglich und ein zusätzlicher Schutz gegenüber Angreifern kann etabliert werden. Der Einsatz von Network Intrusion Detection Systemen (NIDS) ermöglicht es, diesen Schutz für weitere Protokolle und das ganze Netzwerk bereitzustellen (siehe Maßnahme M 23 „Einsatz von IDS“).

Planung und Konzeption

Switches und Router spielen eine zentrale Rolle bei der Vernetzung einer VoIP-Infrastruktur und somit auch bei deren Verfügbarkeit. Für ein Redundanzkonzept bedeutet dies, dass bei hohem Schutzbedarf ebenfalls Switches und Router redundant ausgelegt werden müssen, um deren Ausfall zu kompensieren (M 1). Andernfalls entstehen sogenannte *Single Points of Failure*, die bei einem Ausfall den Verlust des Telefoniedienstes für das Gesamtnetz oder einzelne Teilbereiche zur Folge haben können.

Weiterhin muss gewährleistet werden, dass mögliche Schwachstellen, die bei der Verarbeitung von Protokollen auftreten, durch das Einspielen von Patches beseitigt werden oder entsprechende Maßnahmen ergriffen werden, die ein Ausnutzen der Schwachstelle verhindern (M 13).

Um die Stromversorgung von Switches und Routern bei einem Stromausfall zu sichern sind diese auch durch eine USV-Anlage zu versorgen (M 19). Für die

unterbrechungsfreie Stromversorgung der IP-Telefone (M 20) müssen Switches und Router zusätzlich die Speisung der Endgeräte über PoE unterstützen.

Switches und Router sind wie die IP-Telefonanlage durch eine physische Zutrittskontrolle nach Maßnahme M 21 vor dem unberechtigten Zugriff und der Manipulation zu schützen.

Maßnahmen	Schutzbedarf	
	normal	hoch
M 1 Redundante Auslegung wichtiger Netzkomponenten		X
M 2 Trennung von Sprach- und Datennetz	X	X
M 5 Bandbreitenmanagement	X	X
M 6 Monitoring und Logging	X	X
M 9 Absichern der Remote-Schnittstellen	X	X
M 13 Patchmanagement	X	X
M 15 Sichere Endgeräteauthentifizierung mittels IEEE 802.1X		X
M 18 Absichern der Basis-Netzwerkdienste		X
M 19 USV für die Middleware		X
M 21 Physische Zutrittskontrolle	X	X
M 23 Einsatz von IDS	ZM	ZM

Tabelle 11: Maßnahmen beim Einsatz von Switches und Routern (ZM = Zusatzmaßnahme)

3.2.6 Softphone

Bei einem Softphone handelt es sich um Software, die auf einem Computer installiert wird und durch den zusätzlichen Einsatz eines *Headsets* einen ähnlichen Funktionsumfang wie ein IP-Telefon bietet. Softphones unterscheiden sich wie IP-Telefone durch die unterstützten Protokolle und in den bereitgestellten Leistungsmerkmalen. Ein Softphone ist die logische Konsequenz der Konvergenz von Sprach- und Datennetzwerken und stellt gerade für Heimanwender eine kostengünstige Einstiegsmöglichkeit in die IP-Telefonie dar. Auch in Umgebungen wie *Call-Centern* bieten Softphones zahlreiche Vorteile und werden daher dort regelmäßig eingesetzt. Softphones können als Vermittler zwischen Sprach- und Datennetz aufgefasst werden, da sie auf Computern im Datennetz installiert sind, jedoch zur Vermittlung von Gesprächen Zugriff auf das Sprachnetz benötigen [Hal03, S. 5]. Um die Trennung von Sprach- und Datennetz aufrecht zu erhalten, ist somit ein wesentlich erhöhter administrativer Aufwand nötig.

Gefährdungslage

Beim Einsatz von Softphones werden die folgenden Gefährdungen angenommen.

Gefährdungen
G 1 Abhören von Gesprächen
G 2 Abhören von Räumen mit Endgeräten
G 3 Bekanntwerden von Kommunikationsprofilen
G 4 Unbefugter Zugriff auf Konfigurationseinstellungen
G 5 Ausnutzen von Implementierungsfehlern
G 6 Bekanntwerden interner vertraulicher Informationen
G 7 Gebührenbetrug
G 8 Kompromittierung von Registrierungsinformationen
G 9 Vortäuschung einer Identität
G 10 Verlust und Beeinträchtigung der Verfügbarkeit
G 11 Manipulation von Sprachdaten
G 12 Abstreitbarkeit von Gesprächen
G 16 Kopplung von Ausfallrisiken

Tabelle 12: Gefährdungen beim Einsatz von Softphones

Maßnahmenempfehlung

Die umzusetzenden Maßnahmen sind mit denen des Moduls IP-Telefon bis auf die im Folgenden beschriebenen identisch.

Es entfallen die Maßnahmen zur Absicherung der *Multiportfunktion* (M 10) und zur Sicherstellung der unterbrechungsfreien Stromversorgung (M 20). In Netzwerken mit der Schutzbedarfskategorie hoch sollten Softphones aufgrund der zusätzlichen Risiken nicht eingesetzt werden (M 4). Bei normalen Schutzbedarf müssen die Kriterien der Maßnahme M 3 umgesetzt und eine Trennung von Sprach- und Datennetz aufrechterhalten werden. Die Maßnahme M 11 „Sichere Konfiguration der IP-Telefone“ muss ebenfalls beim Einsatz von Softphones umgesetzt werden.

Maßnahmen	Schutzbedarf	
	normal	hoch
M 3 Sicherer Einsatz von Softphones	X	
M 4 Kein Einsatz von Softphones		X
M 5 Bandbreitenmanagement	X	X
M 6 Monitoring und Logging	X	X
M 7 Verschlüsselung der Signalisierung	X	X
M 8 Verschlüsselung der Sprachdaten	X	X
M 9 Absichern der Remote-Schnittstellen	X	X
M 11 Sichere Konfiguration der IP-Telefone	X	X
M 13 Patchmanagement	X	X
M 14 Authentifizierung der Endgeräte	X	X
M 15 Sichere Endgeräteauthentifizierung mittels IEEE 802.1X		X

Tabelle 13: Maßnahmen beim Einsatz von Softphones

3.3 Checkliste für durchzuführende Maßnahmen

Module	IP-PBX		ISDN-GW		IP-GW		IP-Telefon		Switch/Router		Softphone	
Schutzbedarf (normal = 1, hoch=2)	1	2	1	2	1	2	1	2	1	2	1	2
Maßnahmen												
M 1 Redundante Auslegung wichtiger Netzkomponenten	-	X	-	X	-	X			-	X		
M 2 Trennung von Sprach- und Datennetz									X	X		
M 3 Sicherer Einsatz von Softphones											X	-
M 4 Kein Einsatz von Softphones											-	X
M 5 Bandbreitenmanagement	X	X	X	X	X	X	X	X	X	X	X	X
M 6 Monitoring und Logging	X	X	X	X	X	X	X	X	X	X	X	X
M 7 Verschlüsselung der Signalisierung	X	X	X	X	X	X	X	X			X	X
M 8 Verschlüsselung der Sprachdaten	X	X	X	X	X	X	X	X			X	X
M 9 Absichern der Remote-Schnittstellen	X	X	X	X	X	X	X	X	X	X	X	X
M 10 Absichern der Multiportfunktion							X	X				
M 11 Sichere Konfiguration der IP-Telefone							X	X			X	X
M 12 Einsatz von Profilen für Endgeräte	X	X	X	X	X	X						
M 13 Patchmanagement	X	X	X	X	X	X	X	X	X	X	X	X
M 14 Authentifizierung der Endgeräte	X	X	X	X	X	X	X	X			X	X
M 15 Sichere Endgeräteauthentifizierung mittels IEEE 802.1X							-	X	-	X	-	X
M 16 Absicherung der Netzübergänge zu öffentlichen VoIP-Netzwerken					X	X						
M 17 Absichern der IP-Telefonanlage	X	X	X	X	X	X						
M 18 Absichern der Basis-Netzwerkdienste	-	X	-	X	-	X			-	X		
M 19 USV für die Middleware	-	X	-	X	-	X			-	X		
M 20 USV für IP-Telefone							-	X				
M 21 Physische Zutrittskontrolle	X	X	X	X	X	X			X	X		
M 22 Sicherstellen der Notrufmöglichkeit					X	X						
M 23 Einsatz von IDS	ZM	ZM	ZM	ZM	ZM	ZM			ZM	ZM		
M 24 Maßnahmen gegen automatisierte unerwünschte Werbeanrufe					ZM	ZM						

Tabelle 14: Durchzuführende Maßnahmen (ZM = Zusatzmaßnahme)

3.4 Maßnahmen-Gefährdungstabelle

Maßnahmen	Gefährdungen
M 1 Redundante Auslegung wichtiger Netzkomponenten	G 10
M 2 Trennung von Sprach- und Datennetz	G 16
M 3 Sicherer Einsatz von Softphones	G 7, G 16
M 4 Kein Einsatz von Softphones	G 7, G 16
M 5 Bandbreitenmanagement	G 10
M 6 Monitoring und Logging	G 5, G 8, G 10
M 7 Verschlüsselung der Signalisierung	G 3,G 6, G 7, G 8, G 9, G 10
M 8 Verschlüsselung der Sprachdaten	G 1, G 6, G 10, G 11
M 9 Absichern der Remote-Schnittstellen	G 1, G 2, G 3, G 4, G 5, G 8, G 10
M 10 Absichern der Multiportfunktion	G 16
M 11 Sichere Konfiguration der IP-Telefone	G 1, G 2, G 4, G 6, G 7, G 9
M 12 Einsatz von Profilen für Endgeräte	G 7
M 13 Patchmanagement	G 5, G 7, G 8, G 10
M 14 Authentifizierung der Endgeräte	G 7, G 8, G 9, G 12
M 15 Sichere Endgeräteauthentifizierung mittels IEEE 802.1X	[a]
M 16 Absicherung der Netzübergänge zu öffentlichen VoIP-Netzwerken	G 4, G 5, G 10, G 16
M 17 Absichern der IP-Telefonanlage	G 1, G 5, G 6, G 7, G 8
M 18 Absichern der Basis-Netzwerkdienste	G 1, G 3, G 8, G 9, G 10, G 11
M 19 USV für die Middleware	G 10
M 20 USV für IP-Telefone	G 10
M 21 Physische Zutrittskontrolle	G 1, G 3, G 4, G 8, G 10, G 13
M 22 Sicherstellen der Notrufmöglichkeit	G 15
M 23 Einsatz von IDS	G 1, G 3, G 5, G 10
M 24 Maßnahmen gegen automatisierte unerwünschte Werbeanrufe	G 14

Tabelle 15: Maßnahmen-Gefährdungstabelle

[a] Eine VoIP-spezifische Gefährdung zu dieser Maßnahme existiert in dieser Arbeit nicht. Dennoch ist diese Maßnahme bei hohem Schutzbedarf umzusetzen, um den Zugang zum Netzwerk wirkungsvoll zu kontrollieren. Ferner müssen IP-Telefone bei genutzter Multiport-Funktion ebenfalls die Kontrolle des Netzzungangs durch IEEE 802.1X unterstützen.

4 Gefährdungen beim Einsatz von VoIP

4.1 Gefährdungsübersicht

4.2 Gefährdungen

G 1 Abhören von Gesprächen

Beim Abhören von Gesprächen verbindet die IP-Telefonie sowohl die Gefahren, welche durch den Missbrauch von Leistungsmerkmalen in der Festnetztelefonie existieren[79] als auch solche, die bei einem Abhören von Leitungen in Datennetzen[80] auftreten können. Zusätzlich können Sprachnachrichten abgehört werden, wenn der Abruf der Nachrichten nicht ausreichend abgesichert ist oder der Zugriff auf diese durch eine Schwachstelle[81] ermöglicht wird. Dies hat sowohl im Geschäfts- als auch privatem Umfeld zur Folge, dass Angreifer Zugriff auf vertrauliche Informationen erhalten können.

Die Ursache für das einfache Abhören von Gesprächen in der IP-Telefonie liegt zum einen an der unverschlüsselten Übertragung der Sprachdaten durch das RTP[82]. Andererseits ist im Vergleich zur herkömmlichen Telefonie der technische Aufwand, um ein Gespräch abzuhören, wesentlich geringer. So sind bei der Übertragung von Gesprächen über IP-basierte Netzwerke Lauschangriffe von Rechnern im Netzwerk mit einfachen Mitteln durchzuführen. Die benötigten Tools sind öffentlich und nicht nur autorisiertem Fachpersonal zugänglich. Häufig wird dem Angreifer das Abhören zusätzlich erleichtert, indem der Zugang zum Netzwerk nicht ausreichend abgesichert ist.

Um ein Gespräch im Netzwerk abzuhören, ist es notwendig, dass der komplette Datenstrom aufgezeichnet werden kann. Das ist gegeben, wenn ein Gesprächsteilnehmer und der Angreifer sich in einer Kollisionsdomäne befinden und Pakete eines Absenders an alle angeschlossenen Mitglieder gesendet werden. Eine weitere Möglichkeit ein Gespräch im Netzwerk abzuhören besteht darin, dass der Angreifer Zugang zu einem zentralen Punkt der Infrastruktur besitzt, an dem sämtliche übertragenen Daten zusammen laufen. Diese beiden Möglichkeiten werden auch als passives Abhören bezeichnet, da keinerlei Einfluss auf die Kommunikationsverbindung genommen wird. Beim aktiven Abhören hingegen ist der Angreifer gezwungen, die Kommunikation der Gesprächsteilnehmer über sich umzuleiten. Diese Variante wird auch als MitM-Angriff bezeichnet wodurch die Rolle des Angreifers in diesem Szenario verdeutlicht wird.

[79] [BSI05b, S. 601, G 5.12]
[80] [BSI05b, S.665, G 5.7]
[81] [Poi05, Asterisk Voicemail Unauthorized Access Vulnerability]
[82] Entsprechende Grundlagen des RTP wurden in Kapitel 2.2.4 (RTP & RTCP) besprochen.

G 2 Abhören von Räumen mit Endgeräten

Wie auch herkömmliche Telefone, können VoIP-Endgeräte dazu benutzt werden, Räume, wie beispielsweise ein Büro oder einen Konferenzraum, abzuhören [BSI05b, S. 602, G 5.13]. Mögliche Ansätze bieten dabei die Kompromittierung von IP-Telefonen oder Softphones, der Missbrauch von Managementfunktionen wie Debug-Modi, Schwächen im Protokolldesign, Malware in Verbindung mit Softphones oder der Missbrauch von Leistungsmerkmalen wie die automatische Rufannahme (*Auto-Answer*) und das Freisprechen (*Hands-Free Mode*).

Charakteristisch für diese Angriffe ist, dass sie aus der Ferne ausgeführt werden können und somit zu keinem Zeitpunkt ein direkter physikalischer Zugriff zu dem abgehörten Raum oder dem IP-Telefon bestehen muss. Zudem erfolgt das Abhören im Idealfall ohne besondere akustische und optische Auffälligkeiten des IP-Telefons, so dass die Chance den Angriff zu bemerken mitunter sehr gering ist.

G 3 Bekanntwerden von Kommunikationsprofilen

Wenn die Signalisierung von VoIP-Gesprächen unverschlüsselt erfolgt, können die Daten mit einfachen Mitteln mitgelesen werden. Informationen, die der Angreifer dadurch erhalten kann, sind Teilnehmerkennung der Gesprächspartner (SIP-URI), Uhrzeit, Datum, Dauer des Telefonats und Standortinformationen der Gesprächspartner [EGJ+05, S. 20].

Weiterhin werden die oben genannten Informationen häufig für Abrechnungszwecke gespeichert, um so für jeden Teilnehmer in Form eines Einzelverbindungsnachweis verfügbar zu sein. Desweiteren sind diese Daten bei einigen IP-Telefonen über ein Web-Interface in Form verschiedener Ruflisten verfügbar. Werden die anfangs genannten Informationen nicht ausreichend geschützt, lässt sich mit ihnen ein detailliertes Kommunikationsprofil der Firma und der Mitarbeiter erstellen [BSI98, Kap. 3.2.5].

G 4 Unbefugter Zugriff auf Konfigurationseinstellungen

Beim Einsatz von IP-Telefonen besteht die Gefahr, dass Angreifer die Konfiguration der Endgeräte manipulieren können. Diese Manipulation wird möglich, wenn der Zugang am Endgerät oder über eine Remote-Schnittstelle nicht durch ein Passwort geschützt ist. Weiterhin kann durch die Übertragung von Zugangsdaten im Klartext ein Angreifer Zugriff auf die Konfiguration erhalten. Diese Möglichkeit besteht, wenn die Administration der Endgeräte unverschlüsselt erfolgt.

Beide Ursachen für einen unbefugten Zugriff liegen beim Trivial File Transfer Protocol (TFTP) vor, da zum einen die Übertragung unverschlüsselt erfolgt und

zum anderen der Zugriff auf den Server nicht authentifiziert erfolgt. Dieses Protokoll wird häufig eingesetzt, wenn in großen Umgebungen das Management der IP-Telefone vereinfacht werden soll, indem alle Geräte ihre Konfiguration von einem zentralen Server beziehen.

Mögliche Änderungen der Konfiguration können eine ungewollte Rufumleitung, die Manipulation von Kurzwahlen, die Änderung der Netzwerkeinstellungen und das Deaktivieren oder Aktivieren einer schwächeren Verschlüsselung sein. Der Zugang zu Konfigurationseinstellungen kann ebenfalls dazu missbraucht werden, die in Gefährdung G 2 beschriebenen Leistungsmerkmale, wie eine automatische Rufannahme so zu konfigurieren, dass ein Abhören des Raumes möglich wird. Weitere Folgegefährdungen können Gebührenbetrug oder der Verlust der Verfügbarkeit sein[83].

G 5 Ausnutzen von Implementierungsfehlern

Wie bei bisher eingesetzten Netzwerkprotokollen (HTTP oder SMB), besteht ferner bei VoIP-Protokollen (SIP, H.323) die Gefahr, dass Implementierungsfehler bei der Verarbeitung von Anfragen in Form von *Exploits* ausgenutzt werden können. Dabei werden manipulierte Nachrichten erzeugt, die häufig eine bestimmte Länge eines Datenfeldes (CSeq, SDP) oder eines ganzen Paketes (UDP) überschreiten [JP06, S. 67].

Ein solches Fehlverhalten von Software wird als *Buffer-Overflow* bezeichnet, wenn es möglich ist, die Rücksprungadresse der Funktion so zu beeinflussen, dass das Einschleusen von eigenem Code möglich wird. Dadurch kann ein Angreifer unautorisiert Zugriff zu einem System erlangen, wodurch zahlreiche in diesem Kapitel beschriebene Gefährdungen auftreten können. Ein DoS-Angriff beeinflusst gegenüber einem *Buffer-Overflow* die Verfügbarkeit der Komponente, so dass der Dienst stark beeinträchtigt ist oder mitunter gar nicht mehr verfügbar ist[84]. Neben den Folgen, die von solchen Schwachstellen ausgehen kommt hinzu, dass die Angriffe in den meisten Fällen auch remote ausführbar sind was die Gefahr zusätzlich erhöht.

Auf zahlreiche Implementierungsfehler im SIP machten in der Vergangenheit bereits das CERT im Jahr 2003 [RF03] und die Firma Tele-Consulting GmbH im Jahr 2006 [GL06] aufmerksam.

Auslöser des *Cert-Advisories* war eine Untersuchung der Oulu University Secure Programming Group (OUSPG), die mit Hilfe der „PROTOS Test-Suite“ zahlreiche SIP-Implementationen von unterschiedlichen Herstellern untersucht hatte. Das Resultat des Tests reichte von „*unerwartetem Verhalten des Systems*“ und „*Denial of Service*“ bis zum „*entfernten Ausführen von Code*“ [RF03, Kap. 1].

[83] siehe G 7 „Gebührenbetrug“ und G 10 „Verlust und Beeinträchtigung der Verfügbarkeit“
[84] siehe Gefährdung G 10 „Verlust und Beeinträchtigung der Verfügbarkeit“

Das Advisory der Firma „Tele-Consulting GmbH“ machte auf Schwachstellen in SIP-Nachrichten vom Typ *Notify* aufmerksam. In diesem Fall war es aufgrund von nicht überprüften Feldern in SIP-Nachrichten möglich, mittels *SIP-Spoofing* einen Nutzer auf seinem Display über neue Sprachnachrichten zu informieren. Wird diese Schwachstelle in einer großen VoIP-Umgebung ausgenutzt, kann durch zahlreiche Anfragen an die *Voice-Box* der Dienst überlastet werden. Anschließend versuchen die Nutzer den Support aufgrund der nicht vorhandenen Sprachnachricht zu informieren [GL06].

G 6 Bekanntwerden interner vertraulicher Informationen

Eine weitere Gefährdung ist das Bekanntwerden von Informationen, welche nur für den internen Gebrauch bestimmt sind. Sie können einem Angreifer gezielte Ansatzpunkte für den Angriff auf ein System bieten [Gra01].

Zu kritischen Informationen zählen unter anderem Angaben über eingesetzte Software mit entsprechenden Versionsnummern, Benutzerkonten und Authentifizierungsmechanismen, Informationen zum Aufbau eines Netzwerkes wie IP-Adressen, eingesetzte Hardware wie Herstellernamen von IP-Telefonen, Adressbücher, Ruflisten und Aufenthaltsort oder Anwesenheit eines Mitarbeiters[85]. Möglichkeiten, wie diese Informationen nach außen gelangen können, sind Schadsoftware wie Trojaner, falsch konfigurierte VoIP-Endgeräte[86] und VoIP-Middleware[87] sowie deren Remote-Schnittstellen oder Ansagen von Anrufbeantwortern.

G 7 Gebührenbetrug

Die unberechtigte Inanspruchnahme von Leistungen wird als Gebührenbetrug bezeichnet. Das bedeutet, dass Gespräche auf Kosten anderer geführt werden[88].

Die häufigste Ursache des Gebührenbetrugs liegt darin, dass innerhalb der VoIP-Infrastruktur die Wahlmöglichkeiten der Benutzer nicht ausreichend eingeschränkt sind. So kann ein Benutzer diese Tatsache nutzen, um teure Service-Nummern anzurufen oder ein unbekannter Dritter, um über ein öffentliches Telefon in der Lobby gebührenpflichtige Gespräche zu führen.

Wie in der Festnetztelefonie, können bei der IP-Telefonie Leistungsmerkmale die Ursache für den Gebührenbetrug sein. So kann eine Rufumleitung auf ein Mobiltelefon oder vom Zieltelefon (*Follow-Me-Funktion*) zusätzlich die Kosten erhöhen [BSI98, Kap. 3.2.1].

[85] So kann beispielsweise beim Einsatz des SIP ein Angreifer durch den Erhalt einer *300 Multiple Choices-Antwort* Rückschlüsse auf den Aufenthaltsort des Angerufenen ziehen [AAG+05, S. 49].

[86] IP-Telefone, Softphones (siehe Kapitel 3.2)

[87] IP-Telefonanlage, VoIP-Gateways (siehe Kapitel 3.2)

[88] Der Gebührenbetrug ist kein VoIP-spezifisches Problem. Bereits seit der Einführung der automatischen Ortsvermittlung von AT&T in den 50er Jahren wurde versucht, Wege zu finden kostenfrei zu telefonieren. Populär wurde der Gebührenbetrug in den 70igern unter dem Begriff *Phreaking* [Por06, S. 92].

Im Kontext von VoIP besteht zusätzlich auch die Möglichkeit, dass IP-Telefonanlagen keinerlei Authentifizierungsmaßnahmen umsetzen und jeder beliebige Nutzer ohne Identitätsfeststellung die angebotenen Dienste in Anspruch nehmen kann. Ein Angreifer kann aber auch unberechtigterweise in den Besitz von Zugangsinformationen kommen [BSI98, Kap. 3.2.1]. Eine genauere Beschreibung der Gefahren, die durch die Kompromittierung von Registrierungsinformationen entstehen, ist in der Gefährdung G 8 zu finden.

Mit zunehmender Nutzung von VoIP mittels Softphones wird vermehrt Gebührenbetrug durch Dialer auftreten, die wie in herkömmlichen Telefonnetzen auf Kosten der Nutzer teure Servicenummern anwählen.

In der BSI-Studie VoIPSEC [AAG+05, S. 43] wird zudem auch die Möglichkeit des Gebührenbetrugs durch die Manipulation von zentralen *Accounting-Informationen* genannt. Auf diese Weise lassen sich Leistungsmissbräuche verschleiern und eine korrekte Zuordnung der berechneten Gebühren wird somit unmöglich.

G 8 Kompromittierung von Registrierungsinformationen

Unter Registrierungsinformationen sind Benutzernamen und Passwörter zu verstehen, die zur Authentifizierung von Geräten und Personen eingesetzt werden. Die Kompromittierung derartiger Informationen kann durch unterschiedliche Art und Weise erfolgen.

Zum einen können die Daten bekannt werden, wenn sie unverschlüsselt über das Netzwerk übertragen werden. Außerdem können bei der Verwendung von schwachen Passwörtern diese Daten kompromittiert werden, indem sie über *Brute-Force-* oder Wörterbuch-Angriffe gebrochen werden [JP06, S. 69]. Sollten Default-Passwörter noch aktiv sein, ist es ausreichend das Handbuch zu lesen. Ebenfalls kann es Angreifern gelingen, Zugangsdaten zu kompromittieren, die in einer Datenbank oder direkt auf dem Server in Dateien abgelegt sind (siehe Gefährdung G5 „Ausnutzen von Implementierungsfehlern“). Bestehende Bedrohungen wie Schadsoftware und *Phishing* können zusätzlich die Kompromittierung von Registrierungsinformationen zur Folge haben.

Die IT-Grundschutz-Kataloge machen in der Gefährdung G 3.43 „Ungeeigneter Umgang mit Passwörtern“ darauf aufmerksam, dass Authentifizierungsdaten wie Passwörter, PINs oder Authentifizierungstoken häufig unsachgemäß aufbewahrt oder weiter gegeben werden [BSI05b, S. 478, G 3.43]. Somit ist es Dritten möglich Zugang zu Authentifizierungsdaten zu erhalten und mögliche Folgegefährdungen, wie der Gebührenbetrug (siehe Gefährdung G 7) oder der Identitätsbetrug (siehe Gefährdung G 9), können auftreten.

G 9 Vortäuschung einer Identität

Das Vortäuschen einer Identität beinhaltet, dass ein Angreifer seine wahre Identität verschleiert und versucht, seinem Opfer eine bestimmte Vertrauensbeziehung vorzutäuschen [JP06, S. 60]. Diese Vertrauensbeziehung basiert im allgemeinen auf einer Absenderadresse. Wenn es einem Angreifer gelingt, diese nachzuahmen (*Spoofing*), er in den Besitz der zugehörigen Zugangsdaten kommt oder er die Möglichkeit hat, von einem vertrauenswürdigen Anschluss (Telefon) anzurufen, kann er erfolgreich seine wahre Identität verbergen. Diese Vertrauensbeziehung kann dann missbraucht werden, um an sensible Informationen zu kommen oder Dienste auf fremde Kosten in Anspruch zu nehmen.

Eine Ausprägung der Identitätsfälschung tritt vermehrt bei E-Mails auf und wird als *Phishing* bezeichnet. Dabei wird versucht, über plausible Darstellungen unter Vorgabe einer falschen Identität vertrauliche Informationen, wie Zugangsdaten oder TANs, zu erschleichen. Dieses Vorgehen ist ebenso auf VoIP übertragbar und wird dann als *Vishing* bezeichnet. Die Firma „Secure Computing“ machte bereits in einer Pressemitteilung auf einen *Vishing-Angriff* aufmerksam [Bac06]. Dort wird ein prinzipieller Beispielablauf eines *Vishing-Angriffs* erläutert. Zunächst werden mit Hilfe eines *Wardialers* zahlreiche Anrufe in einer bestimmten Region vorgenommen. Wenn der Anschlussinhaber einen solchen Anruf annimmt, hört er eine Bandansage, die auf betrügerische Aktivitäten seiner Kreditkarte aufmerksam macht und eine Servicenummer zur weiteren Klärung angibt. Wenn das potenzielle Opfer die angegebene Rufnummer anruft, wird über eine scheinbare Verifikation seiner Person mittels Kreditkartennummer versucht diese zu erhalten. Dadurch besitzt der Angreifer ausreichend Informationen (Telefonnummer, Name, Adresse und Kreditkartennummer), um Kreditkartenbetrug zu begehen. Die initiierte Vertrauensbeziehung kann dann ausgenutzt werden, um zusätzliche vertrauliche Informationen wie PIN, Ablaufdatum, Geburtsdatum und Kontonummer zu erhalten [Bac06].

G 10 Verlust und Beeinträchtigung der Verfügbarkeit

Der Verlust der Verfügbarkeit bedeutet in diesem Zusammenhang, dass der Dienst der IP-Telefonie nicht mehr zur Verfügung steht. Dies kann je nach Ursache einzelne Nutzer, Gruppen von Nutzern oder durch den Ausfall einer zentralen Komponente alle Nutzer einer Infrastruktur betreffen. Wenn die IP-Telefonie nicht mit den gewohnten Qualitätsmerkmalen zu Verfügung steht, liegt eine Beeinträchtigung der Verfügbarkeit vor. Für den Nutzer kann dies im Einzelfall kurzzeitige Aussetzer oder eine schlechte Übertragungsqualität während des Telefonats zur Folge haben [AAG+05, Kap. 3.1.3].

Der Verlust beziehungsweise die Beeinträchtigung der Verfügbarkeit sind als eine Folgegefährdung zu betrachten, da jeder dieser Situationen die Ausnutzung einer Schwachstelle vorausgeht. Im Folgenden sollen einige Gefährdungen aufgezeigt

werden, die die Verfügbarkeit in einem VoIP-Netzwerk einschränken können oder den Verlust dieser zur Folge haben.

- DoS-Angriff gegen VoIP-Endgeräte
- DoS-Angriff gegen Netzwerk-Basisdienste
- Hardwaredefekt
- Softwarefehler
- Stromausfall
- Unterbrechen von Telefonaten (engl. *Call Teardown*)[89] [EGJ+05, Kap. 8.1.1.4.1].
- Umleiten von Anrufen (engl. *Registration Hijacking*) [RSC+02, Kap. 26.1.1].

G 11 Manipulation von Sprachdaten

Sprachdaten können auf verschiedene Art und Weise manipuliert werden. Ein Angreifer kann ein Gespräch abhören und dessen Inhalt in Echtzeit verändern. Wenn einzelne Wörter verloren gehen oder hinzugefügt[90] werden, kann der Inhalt des Gespräches missverstanden werden [Mat06, Abs. Service Integrity]. Ebenso ist eine Manipulation von Sprachnachrichten während der Aufnahme als auch im Nachhinein auf einer Mailbox möglich, sofern der Angreifer Zugriff zu dem System hat.

G 12 Abstreitbarkeit von Gesprächen

Formal gesehen werden zwei Formen von Abstreitbarkeit unterschieden. So kann ein Empfänger den Erhalt der Nachricht leugnen und der Absender bestreiten, dass er eine Nachricht verschickt hat [BSI05b, S. 1770, M 3.23].

Abstreitbarkeit spielt häufig dann eine Rolle, wenn Nutzer die Möglichkeit haben, die Verwendung von Diensten zu leugnen und gestellte Rechnungen anzufechten [AAG+05, S. 103]. Dadurch ist es bei VoIP notwendig, dass Anbieter die Verbindlichkeit der Dienstnutzung gegenüber Dritten sicherstellen können. Somit kann Nutzern nachgewiesen werden, dass sie einen Dienst zu einem bestimmten Zeitpunkt in Anspruch genommen haben.

[89] *BYE-Anfrage* bei SIP

[90] Bei Verwendung des RTP ist es möglich Pakete in den RTP-Strom einzufügen und somit die Semantik einer Aussage entscheidend zu verändern (siehe *Insertion Attack* in Kapitel A.3.2 Protokollspezifische Angriffe).

G 13 Unbefugter Zutritt zu Basiskomponenten

Wie auch bei anderen IT-Systemen kann auch eine Gefahr von Personen ausgehen, die unbefugt Zugang zu Basiskomponenten wie Servern, Endgeräten und der Netzinfrastruktur erhalten [EGJ+05, Kap. 8.2]. Die IT-Grundschutz-Kataloge nennen in diesem Zusammenhang[91] vorsätzliche Handlungen oder unbeabsichtigtes Fehlverhalten als mögliche Ursachen. Diese können je nach betroffener Netzkomponente einen Ausfall einzelner Bereiche, einen Totalausfall oder die Kompromittierung des ganzen VoIP-Systems bedeuten. Bei vorsätzlicher Handlung ist die Kompromittierung der VoIP-Basiskomponenten ebenfalls durch ungesicherte Managementschnittstellen denkbar. Durch einen ungesicherten Zugang zum Netz besteht zudem die Möglichkeit, dass die Kommunikation der VoIP-Teilnehmer abgehört werden kann.

G 14 Unerwünschte Werbeanrufe

Spam over Internet Telephony (SPIT) bezeichnet unerwünschte Werbeanrufe, ähnlich wie bei E-Mail, in denen Nutzer mit ungewollten Werbenachrichten überflutet werden. Aufgrund zahlreicher Parallelen zur E-Mail ist zu erwarten, dass SPIT in Zukunft ähnlich problematisch wie SPAM wird und die Mailboxen der Anwender durch Werbebotschaften gefüllt werden.

Zu den Ursachen von SPIT zählen, dass die Kosten der Anrufe vernachlässigbar, technische Barrieren gering sind und wie bei der E-Mail zahlreiche Anrufe automatisiert getätigt werden können [Dav06]. Eine weitere Parallele zur E-Mail ist die Nutzer-zu-Nutzer-Kommunikation bei VoIP. Diese macht es für Werbende interessant, Angebote über VoIP zu verbreiten [RJP06, Abs. Abstract].

Es kann davon ausgegangen werden, dass SPIT ähnlich zum Alltag gehören wird wie SPAM, da eine Unterdrückung von Anrufen nach §§ 148f. TKG problematisch ist [RTH+06, Kap. 4.1.2]. Im Gegensatz zum *Store-and-Forward-Prinzip* bei E-Mails, wird die Erkennung von SPIT durch die Echtzeitkommunikation bei VoIP wesentlich erschwert und eine Filterung des Inhaltes unpraktikabel [RJP06, Kap. 3.2].

Aktuell hat eine Bedrohung durch SPIT keine große Bedeutung. Das liegt vor allem daran, dass bestehende VoIP-Netzwerke häufig sogenannte Insellösungen sind, die in Intra- oder Extranets eingesetzt werden und somit keine Ende-zu-Ende-Kommunikation durch VoIP stattfindet. Da eine Erreichbarkeit hierbei nur über das herkömmliche Telefonnetz gegeben ist, wird die kostengünstige Verbreitung von Werbung hinfällig. Diese Konstellation von Insellösungen ist jedoch nur zeitlich bedingt und mit einer zunehmenden Akzeptanz und Umsetzung von Sicherheitsmechanismen wird eine Erreichbarkeit aus dem Internet über Protokolle wie SIP gegeben sein [RJP06, Kap. 1].

[91] [BSI05b, S. 303, G 2.6]

G 15 Fehlende oder eingeschränkte Notrufmöglichkeit

Erhebliche Einschränkungen im Bereich VoIP liegen bei der Bereitstellung einer Notrufmöglichkeit vor. Diese ist von Anbietern in vollem Umfang[92] nicht verfügbar. Folglich kann ohne einen TK-Basisanschlusses keine zufriedenstellende Notrufmöglichkeit zur Verfügung gestellt werden.

Weiterhin existieren aktuell keine gesetzlichen Vorgaben für die Bereitstellung der Notruffunktionalität bei VoIP [TAO06a, S. 39]. Die gesetzlichen Anforderungen nach §108 TKG 2004, die unter anderem für die Festnetztelefonie gelten, sind wie folgt zusammenzufassen. Erbringer öffentlich zugänglicher Telefondienste sind verpflichtet Notrufmöglichkeiten bereitzustellen und Notrufe unter Angabe der Rufnummer des Anschlusses und der Daten zur Standortermittlung zur nächsten zuständigen Notrufabfragestelle zu vermitteln [BI04].

Hauptproblem ist dabei die Ermittlung einer geografischen Region um eine Notrufabfragestelle und den Standort des Notrufenden zu bestimmen. Ein fester Bezug zwischen Rufnummer und Adresse eines Anschlusses, wie bei der Festnetztelefonie, ist nicht gegeben. Zudem besteht der Anspruch, dass die Bereitstellung der Notruffunktionalität unabhängig vom Standort des Notrufenden ist [TAO06a, S. 39]. Die Lokalisierung des Notrufes erfordert auch einen Datenaustausch zwischen denen am Prozess beteiligten Netzbetreibern. Dafür sind rechtliche Regelungen für den Datenaustausch zwischen Providern, Schnittstellenspezifikationen und einheitliche Datenformate notwendig [TAO06b, S. 27].

G 16 Kopplung von Ausfallrisiken

Werden Sprach- und Datennetz in einem Subnetz betrieben, können sich Gefährdungen, wie DoS-Angriffe und Schadsoftware, die von herkömmlichen Datennetzen ausgehen, negativ auf die Sicherheit des Sprachnetzes auswirken. Die Ursache der Kopplung von Ausfallrisiken kann einerseits die gemeinsam genutzte Infrastruktur wie ein DHCP-Server sein oder der direkte Angriff eines infizierten Computers auf ein VoIP-Endgerät. Ebenso besteht die Möglichkeit, dass keine ausreichende Dimensionierung der Internetanbindung gegeben ist und es somit bei erhöhter Netzlast zu Engpässen und daraus resultierenden Paketverzögerungen sowie Paketverlusten kommen kann. Andererseits können sich die in diesem Kapitel erwähnten Gefährdungen negativ auf die Sicherheit des Datennetzes auswirken.

[92] Eine standortunabhängige sogenannte *Röchelruf-Lösung*, bei der der Notrufende keine Informationen übermitteln kann, ist bisher nicht verfügbar [SIP05].

5 Maßnahmen zur Absicherung

5.1 Maßnahmenübersicht

5.2 Maßnahmen

M 1 Redundante Auslegung wichtiger Netzkomponenten

Gerade bei zeitkritischen Anwendungen wie der IP-Telefonie und deren Verfügbarkeitsanforderungen, ist es notwendig Redundanz zu schaffen, um so mögliche Ausfallzeiten, Qualitätseinbußen und Kosten durch den Ausfall von Hardware so gering wie möglich zu halten.

Eine adäquate Verfügbarkeit des Telefondienstes gehört zu den wichtigsten Anforderungen an die IP-Telefonie. Die Verfügbarkeit der IP-Telefonie lässt sich steigern, indem entsprechende Netzkomponenten redundant ausgelegt werden und mehrere Zugriffspfade für die Endgeräte existieren. Dies ermöglicht den Ausfall einzelner Komponenten zu kompensieren und das Geschäftsrisiko eines nicht verfügbaren Telefoniedienstes zu minimieren[93].

Bei der Entscheidung, welche Netzkomponente redundant ausgelegt werden sollte, ist die BSI-Studie VoIPSEC hilfreich. Dort werden die „*Komponenten einer VoIP-Umgebung in der Reihenfolge steigender Anforderungen an die Geschwindigkeit der Umschaltung beim Ausfall einer Komponente aufgelistet [...]*“ [AAG+05, S. 79 ff.].

- DHCP-Server, TFTP-Server, FTP-Server
- Registrars oder Gatekeeper
- Provisioning-Server
- Firewall
- Switches und Router
- VoIP-Gateway

Neben den aktiven Netzkomponenten müssen externe Komponenten wie USV-Anlagen und Leitungen beim Redundanzkonzept ebenfalls berücksichtigt werden.

Bei der IP-Telefonie können einige Redundanzkonzepte angewendet werden, die bereits in Datennetzen erfolgreich umgesetzt werden. Zudem existieren Konzepte speziell für die Übertragung von Sprache. Diese sorgen dafür, dass beim Ausfall zentraler Komponenten Gespräche über deren redundant ausgelegte Komponente übertragen werden. Im Folgenden sollen einige Möglichkeiten genannt werden, die zu einer höheren Verfügbarkeit beitragen.

[93] Mögliche Architekturen für die redundante Auslegung der Netzkomponenten sind der Maßnahme M 2.314 „Verwendung von hochverfügbaren Architekturen für Server“ der IT-Grundschutz-Kataloge zu entnehmen.

- Redundante, physikalisch getrennte Verbindung zum Internet-Service-Provider (ISP).
- Redundante Auslegung der Server, die Basis-Netzwerkdienste (z.B. DHCP) anbieten.
- Bereithalten von Festnetz-Leitungen als Backup, um beim Ausfall der Internetanbindung den Telefoniedienst aufrecht zu erhalten.
- *DNS SRV Records* ermöglichen den Endgeräten mehrere Proxy-Server bekannt zu machen, so dass diese einen Proxy anhand der Priorität auswählen und gegebenenfalls beim Ausfall auf einen anderen ausweichen können [RS02a].
- Einführung des Virtual Router Redundancy Protocol (VRRP) (RFC 3768) für zentrale Router[94].
- Herstellerspezifische Hochverfügbarkeits-Lösungen, die den Aufbau redundanter Strukturen mit *Fail-Over-Mechanismen* ermöglichen.

M 2 Trennung von Sprach- und Datennetz

Eine der wesentlichen Vorteile von konvergierenden Sprach- und Datennetzen ist deren mögliches Einsparpotenzial sowie eine Vereinfachung der Administration und des Managements. Dennoch verdeutlicht Gefährdung G 16, dass eine logische oder physikalische Trennung von Sprach- und Datennetz notwendig ist, um einer Kopplung von Ausfallrisiken entgegenzuwirken.

Für Firmen ist es zudem einfacher, QoS-Mechanismen für VoIP-Systeme umzusetzen, wenn diese vom Datennetz getrennt sind. Auch die Sicherheitseinstellungen bei Komponenten wie Firewalls lassen sich einfacher umsetzen, wenn die Rechte für Sprach- und Datensegmente separat definiert werden können [JP06, S. 129].

Neben der in dieser Maßnahme beschriebenen Netztrennung für den Endgerätezugang ist für die beiden Netzsegmente ein eigenes Subnetz mit einem privatem Adressbereich nach RFC 1918[95] zu definieren [DIS06, Kap. 3.5.1].

Häufig ist eine strikte Trennung von Sprach- und Datennetz nicht realisierbar, da IP-Telefone Verzeichnisdienste des Datennetzes nutzen, aus dem Datennetz zur Administration auf das Sprachnetz zugegriffen werden muss oder Sprachnachrichten per E-Mail zugestellt werden. In solchen Umgebungen ist es notwendig, das Sprach- und Datennetz durch den Einsatz von Routern zu vernetzen. Dabei ist es

[94] VRRP fasst mehrere physikalische Router unter einem virtuellen Router zusammen und macht diesen den Endgeräten, in Form einer virtuellen IP-Adresse verfügbar. Beim Ausfall des *Master-Routers* kann die Rolle an andere Router delegiert werden [Hin04].

[95] [RMKGEL96]

jedoch erforderlich, die Netztrennung durch den Einsatz von Firewalls aufrecht zu erhalten, so dass nur Daten ausgetauscht werden können, die zum Betrieb der beschrieben Dienste notwendig sind.

logische Trennung

Die logische Trennung lässt sich mit den im IEEE-Standard 802.1Q[96] spezifizierten Virtual Local Area Networks (VLAN) realisieren. Der Einsatz von VLAN bietet die Möglichkeit, logische Gruppen, sogenannte virtuelle Broadcastdomänen, über ein oder mehrere Switches hinweg zu bilden. Es werden Mechanismen bereit gestellt, Endgeräte unabhängig von ihrem Standort hinzufügen, zu entfernen oder umzugruppieren [LS03, Kap. 1.2]. Die Zugehörigkeit eines *Ethernet-Paketes* zu einer logischen Gruppe (VLAN) wird durch eine VLAN-ID (VID) festgelegt [LS03, Kap. 9.1].

Endgeräte in einem VLAN können nur untereinander kommunizieren. *Broadcast* und *Multicast-Nachrichten* werden ebenfalls nur innerhalb des jeweiligen VLANs weitergeleitet [LS03, Kap. 1.2]. Dies ermöglicht die strikte Trennung von Daten- und Sprachverkehr innerhalb eines konvergenten Netzwerkes. Durch den Einsatz von VLANs können Netzwerke wesentlich besser skaliert werden und eine erhöhte Netzlast durch *Broadcast-Nachrichten* reduziert werden.

physikalische Trennung

Sprach- und Datennetz können auch, sofern es die räumlichen Gegebenheiten es ermöglichen, physikalisch getrennt werden. Dabei werden Endgeräte des Sprach- und Datennetzes direkt auf unterschiedlichen Switches vernetzt.

Wenn im Sprach- oder Datennetz besonders sensible Daten übertragen werden, sollte eine komplette physikalische Trennung der Netzwerke realisiert werden. Die BSI-Studie VoIPSEC nennt in diesem Zusammenhang das Beispiel der Polizei, bei der aufgrund des sehr hohen Schutzbedarfs eine physikalische Trennung notwendig ist [AAG+05, S. 73].

M 3 Sicherer Einsatz von Softphones

Aufgrund der geringeren Kosten gegenüber IP-Telefonen werden häufig Softphones eingesetzt. Dabei sollten jedoch der Funktionsumfang und die sicherheitsrelevanten Eigenschaften der Softphones untersucht werden, um eine den Anforderungen angemessene und sichere Integration in das Netzwerk zu gewährleisten. Eine Hilfestellung für die zu untersuchenden Merkmale ist im Prüfkriterium P 3 „Sicherer Einsatz von Softphones“ zu finden.

Um die in Maßnahme M 2 beschriebene Trennung von Sprach- und Datennetz aufrecht zu erhalten, darf der Zugriff von Computern aus dem Datennetz auf das Sprachnetz nicht möglich sein. Um dies zu gewährleisten, besteht die

[96] [LS03]

Möglichkeit eine Netzwerkkarte und ein Softphone einzusetzen, welche die Trennung von Sprach- und Datenverkehr durch die Vergabe von VLAN-Tags ermöglichen [DIS06, S. 43]. Alternativ kann die Trennung erreicht werden, indem für das Sprach- und Datennetz verschiedene Netzwerkkarten zum Einsatz kommen [DIS06, S. 43]. Das Risiko eines Übergriffs von einen kompromittierten Rechner in das Sprachnetz kann jedoch nicht ausgeschlossen werden. Um die Gefahr zu minimieren, sind zusätzlich Personal-Firewalls und Anti-Virenprogramme einzusetzen.

M 4 Kein Einsatz von Softphones

Im Rahmen dieser Maßnahme ist sicherzustellen, dass Softphones im Netzwerk nicht zum Einsatz kommen. Grund für die Umsetzung der Maßnahme ist, dass Risiken ausgeschlossen werden sollen, die durch den Einsatz von Softphones entstehen. Dazu gehört, dass bei einer Kompromittierung des Computers Daten wie Ruflisten und Passwörter, die auf dem Computer gespeichert werden, nicht in falsche Hände gelangen können. Zusätzlich kann die Gefahr, dass ein Computer durch eine Schwachstelle im Softphone oder bei der Verarbeitung von VoIP-Protokollen kompromittiert wird, durch die Umsetzung dieser Maßnahme ebenfalls ausgeschlossen werden [DIS06, Kap. 3.6].

Ferner muss durch eine Firewall sichergestellt werden, dass Softphones sich nicht zu Servern außerhalb des betreuten Netzwerkes verbinden können. Durch die Trennung von Sprach- und Datennetz und den Einsatz von Firewalls (siehe M 2), sollte es Nutzern nicht möglich sein, ein Softphone in Verbindung mit der internen IP-Telefonanlage zu nutzen.

M 5 Bandbreitenmanagement

Um jedem Gespräch im betreuten Netzwerk die notwendige Bandbreite zur Verfügung zustellen ist es notwendig dass, bei der Einführung von VoIP eine Bandbreitenplanung vorgenommen wurde. Ferner muss die benötigte Bandbreite auch nachhaltig durch Maßnahmen zum Bandbreitenmanagement sichergestellt werden, um somit die Übermittlungszeit der IP-Pakete (*Delay*), mögliche Schwankungen (*Jitter*) sowie Paketverluste zu minimieren. Ein Begriff, der die Anforderungen an das Bandbreitenmanagement zusammenfasst ist die Dienstgüte, auch Quality of Service (QoS) genannt. In der Fachliteratur wird jedoch unterschieden zwischen QoS und Class of Service (CoS). Während bei der QoS eine bestimmte Dienstgüte garantiert wird, werden bei der CoS „*Maßnahmen zur Zuordnung einer bestimmten Dienstgütenkategorie [beschrieben]*“ [AAG+05, Kap. 3.3.4].

Im Folgenden soll auf die wichtigsten CoS- und QoS-Maßnahmen eingegangen werden. Der Einsatz dieser Verfahren muss jedoch abhängig von der jeweiligen Netzstruktur und den Anforderungen individuell entschieden werden[97]. Zusätzlich

[97] „*The recommendation for switched networks is to use IEEE 802.1p/Q. The recommendation*

sollte durch die IP-Telefonanlage sichergestellt werden, dass die mögliche Anzahl von gleichzeitigen Gesprächen nicht überschritten werden kann.

Overprovisioning

Eine Möglichkeit Paketverluste und Verzögerungen in VoIP-Netzwerken zu vermeiden, stellt das Overprovisioning dar. Dabei findet keine Garantie einer bestimmten Dienstgüte statt, sondern es wird davon ausgegangen, dass die Bandbreite ausreichend überdimensioniert ist. Diese Strategie erfordert jedoch ein ausführliches Monitoring von möglichen Engpässen, wie sie bei nicht genügend CPU-Kapazität und Datendurchsatz entstehen können. Ein Richtwert, der beim Overprovisioning angenommen werden kann, ist dass ein über 5 Minuten gemittelter Datendurchsatz 17 bis 25 Prozent der vollen Link-Datenrate belegt [AAG+05, S. 82].

Differentiated Services (DiffServ)

Eine Möglichkeit für die Umsetzung von CoS bieten die Differentiated Services (DiffServ). Dabei werden IP-Pakete unter Verwendung des DS-Feldes[98] im IP-Header markiert und entsprechend ihrer Klassifizierung, der sogenannten Per-Hop-Behavior (PHB), in Netzknoten wie Routern bevorzugt behandelt.

Eine der wichtigsten Aufgaben von CoS-Architekturen wie DiffServ ist die korrekte Verwendung der vorgesehen Mechanismen, so dass keine Pakete unberechtigter Weise mit höheren Prioritäten versehen werden [AAG+05, S. 82]. Somit soll durch CoS-Architekturen wie DiffServ (RFC 2475) sichergestellt werden, dass die Klassifizierung durch die PHB beim Transport der Pakete über die Netzwerkknoten hinweg eingehalten wird (*Policing*) [BBC+98, Kap. 2.3].

IEEE 802.1Q/p

Eine weitere Möglichkeit der Priorisierung von Paketen (CoS) bietet der IEEE-Standard 802.1p (aktuell 802.1D[99]) auf Schicht 2 des ISO/OSI-Referenzmodells. Durch die Klassifikation des Netzwerkverkehrs in *Ethernet-Frames* ist dieser Mechanismus unabhängig gegenüber CoS-Mechanismen auf IP-Ebene, wie den zuvor beschriebenen DiffServ [FS99, S. 83].

---

for routed networks is to use DiffServ Code Points (DSCP). The recommendation for mixed networks is to use both“ [Por06, S. 381].

[98] Das DS-Feld wird in RFC 2474 spezifiziert und ersetzt die Definitionen des IPv4 TOS-Feldes in RFC 791. Es besteht aus dem 2 Bit CU-Feld und dem 6 Bit großen DSCP-Feld, das über seinen Wert (0-64) die Zuordnung von IP-Paketen zu einzelnen Klassen, einer sogenannten Per-Hop-Behavior (PHB), ermöglicht [NBBB98, Kap. 3].

[99] Der Standard 802.1p ist ursprünglich ein eigener Standard gewesen und wird in zahlreichen Datenblättern von IP-Telefonen auch noch unter dieser Bezeichnung geführt. Seit 1998 ist er allerdings Bestandteil des IEEE-Standards 802.1D und wird in der aktuellen Version (802.1D-2004) unter anderem im Kapitel 6.3 „Quality of Service maintenance“ und *Annex G* definiert [JCS04b; FS99].

Bei 802.1Q/p werden 3 Bit des im VLAN-Standard (802.1Q) definierten TCI-Feldes[100] (16 Bit) genutzt, um 8 Prioritäten (*user priorities*) zu vergeben. Innerhalb von 802.1D [JCS04b, Kap. Annex G] wird definiert, wie diese einzusetzen sind. Bei der Priorität 0 handelt es sich um den Standardwert und bei 7 um die höchste Priorität. Anhand der Prioritäten wird hierbei der Netzwerkverkehr seinen Anforderungen entsprechend klassifiziert. Für die Übertragung von Sprache mit weniger als 10 ms Latenz empfiehlt der Standard 802.1D die zugehörige Priorität 6 [JCS04b; LS03].

Integrated Services (IntServ)

Bei den Integrated Services (IntServ) wird eine Garantie der Dienstgüte ermöglicht, indem eine Ende-zu-Ende-Signalisierung durch das Resource Reservation Protocol (RSVP) erfolgt. Dies erfordert jedoch eine Umsetzung der IntServ von allen an der Kommunikation beteiligten Netzknoten. Aufgrund der mangelnden Unterstützung in Endgeräten spielt es in VoIP-Infrastrukturen keine Rolle [AAG+05, S. 83].

MPLS

QoS-Maßnahmen können auch durch das Multiprotocol Label Switching (MPLS) in VoIP-Netzen umgesetzt werden. MPLS ist dabei nicht auf IP-Netze (paketorientiert) begrenzt, sondern kann ebenfalls in ATM-Netzen[101] (leitungsvermittelnd) verwendet werden. MPLS eignet sich für Netzwerke, die ein hohes Aufkommen an Echtzeitdaten haben. Der Einsatz von MPLS empfiehlt sich in Provider- und großen Unternehmensnetzwerken mit mehreren tausend Endgeräten [Wal05, Kap. 9.5.2].

Innerhalb von MPLS bekommt jedes Paket ein *Label* und eine fest definierte Route zugewiesen. Dieser Mechanismus (*Labeling*) wird angewendet, um die Komplexität beim Routing zu reduzieren. Für den weiteren Transport ist kein aufwendiges inspizieren der IP-Pakete auf dem Weg zum Ziel notwendig. Damit dies beibehalten werden kann, stellt MPLS ebenfalls CoS- und QoS-Mechanismen wie die Unterstützung der DiffServ und IntServ bereit. Durch den Einsatz von *Labels* können auch verschiedene Routen für unterschiedliche Protokolle zum selben Ziel definiert werden. Ein solches QoS-Routing ermöglicht die gezielte Wahl einer Route bezüglich der Dienstgüte, die für den Transport der jeweiligen Daten erforderlich ist [FS99].

M 6 Monitoring und Logging

Das Monitoring und Logging ermöglicht einen Überblick über den Zustand der einzelnen Systeme und den des Netzwerkes zu erhalten. Existieren bereits Monitoring- und Loggingmechanismen für das Datennetz, sind diese auf die gesamte Netzwerkinfrastruktur anzuwenden. Dabei muss sichergestellt werden, dass

[100] Tag Control Information (TCI)
[101] Asynchronous Transfer Mode (ATM)

alle Netzkomponenten kompatible Verfahren zur zentralen Protokollierung besitzen. Eine regelmäßige Auswertung der Protokolldaten gewährleistet, dass Vorfälle wie Angriffe, Konfigurationsfehler, Fremdgeräte, Ausfälle oder Performanceengpässe bemerkt werden. Der Einsatz spezieller Software erleichtert die Auswertung in großen Umgebungen und bietet die Möglichkeit der Benachrichtigung bei kritischen Ereignissen. Um eine Manipulation der Protokolldaten auszuschließen und die Zuverlässigkeit zu steigern, ist beim Einsatz von Monitoring- und Loggingmechanismen die Integrität und Authentizität der übertragenen Daten sicherzustellen.

Syslog

Eine Möglichkeit für die Protokollierung von Ereignissen einzelner Systeme bietet das Syslog-Protokoll[102]. Zum einen können mit Hilfe des Syslog-Dienstes die Ereignisse eines Rechners lokal abgelegt werden. Zusätzlich dazu können alle Protokolldaten einzelner Systeme über das Netzwerk an einen zentralen Syslog-Dienst übermittelt werden [Lon01, Kap. 1].

In beiden Fällen können die Daten durch weitere Tools ausgewertet und für bestimmte Ereignisse Benachrichtigungen per E-Mail oder SMS versandt werden. Dabei muss beachtet werden, dass die Übertragung der Logdaten im Netzwerk unverschlüsselt über das UDP erfolgt und daher abgesichert werden sollte. Eine solche Absicherung des Syslog-Dienstes ist durch das RFC 3195[103] vorgesehen. Dieses benennt die Algorithmen, die zum Schutz von Integrität, *Reply-Angriffen*, Authentizität und Vertraulichkeit der Nachrichten eingesetzt werden. Damit die Verfahren zur Verschlüsselung angewendet werden können, ist eine verbindungsorientierte Übertragung der Daten über das TCP vorgesehen [NR01, Kap. 5.1].

SNMP

Einen ähnlichen Ansatz wie Syslog verfolgt das Simple Network Management Protocol (SNMP). Dieses erlaubt den Austausch von Management- und Statusinformationen zur Überwachung und Verwaltung von Netzwerkkomponenten, wie beispielsweise VoIP-Endgeräten. In der ersten Version des SNMP (SNMPv1) wurden dazu verschiedene Typen von SNMP-Nachrichten definiert. Diese können eingesetzt werden, um Informationen oder Konfigurationsänderungen anzufordern oder auf solche Anfragen zu antworten. Über diese Nachrichten können ebenfalls kritische Ereignisse wie Fehler von Endgeräten übertragen werden, sogenannte *Traps*. Die Nachrichten des SNMP werden in ASN.1 kodiert und über das UDP übertragen [CP000].

[102] RFC 3164 [Lon01]
[103] [NR01]

SNMPv1 und SNMPv2 weisen ähnliche Schwächen bezüglich der Authentifikation und der Integrität wie Syslog-Nachrichten auf. Diese wurden durch die aktuelle Version SNMPv3 beseitigt, so dass nun die Integrität, Authentifizierung und Vertraulichkeit der Daten gegeben ist. Zudem bietet SNMPv3 Schutz vor *Reply-Angriffen* [BW02].

M 7 Verschlüsselung der Signalisierung

Viele der in Kapitel A.3.2 aufgelisteten Angriffe beruhen auf einer unverschlüsselten Signalisierung. Um diese gegenüber Dritten gegen Gefährdungen wie Abhören, Anrufprotokollierung und Manipulation abzusichern, ist die verschlüsselte Übertragung der Signalisierung durch eines der im Folgenden genannten Protokolle sicherzustellen.

TLS

Bei TLS handelt es sich um eine sogenannte *Hop-by-Hop-Verschlüsselung*. Hierbei wird die Kommunikation zwischen den an der Übertragung beteiligten Netzkomponenten (Hops) jeweils mit separaten Schlüsselmaterial in einer TLS-Verbindung abgesichert. Diese Vorgehensweise setzt einen vertrauenswürdigen nächsten Hop voraus. Eine Garantie, dass die Verbindung Ende-zu-Ende mit TLS gesichert ist, d.h jede beteiligte Netzkomponente TLS einsetzt, kann dabei nicht gegeben werden [RSC+02, Kap. 26.2.1].

Die Verwendung von SIP in Verbindung mit TLS wird als SIP Secure (SIPS) bezeichnet ähnlich dem HTTPS, bei dem durch den Einsatz von TLS eine sichere Übertragung zwischen Webserver und Webclient hergestellt wird. Jede standardkonforme Implementation muss TLS zur Absicherung der Signalisierung unterstützen und mindestens die *Cipher-Suite* TLS_RSA_WITH_AES_128_CBC_SHA nach RFC 3268 umsetzen[104]. Der Einsatz von TLS ist an dem neuen Schemata SIPS (sips.bob@biloxi.com) in der URI zu erkennen. Die Verwendung von SIPS unterscheidet sich weiterhin gegenüber der herkömmlichen Kommunikation mit SIP durch die Verwendung des verbindungsorientierten Transportprotokolls TCP und des Ports 5061. Innerhalb des *Via-Feldes* wird zusätzlich zur Protokollbeschreibung der Parameter *TLS* als zu verwendendes Transportprotokoll angegeben. Die Verwendung des URI-Schemas SIPS bedeutet für die beiden Kommunikationspartner, dass die Übertragung der SIP-Nachrichten vom Sender zum Empfänger mit TLS abgesichert ist. Eine Ausnahme ist der letzte Hop vom Proxy zum User Agent (UA), bei dem eine adäquate Verschlüsselung eingesetzt werden soll. In [JP06] wird das Beispiel der Verschlüsselung von Wi-Fi Protected Access (WPA) in Verbindung mit einem WLAN-Client angeführt [RSC+02; JP06].

[104] Diese gibt an, welches Schlüsselaustauschprotkoll (RSA), welcher Verschlüsselungsalgorithmus mit welcher Schlüssellänge in welchem Modus (AES_128_CBC) und welches *Hashverfahren* (SHA) angewendet wird [RSC+02, Kap. 26.2.1].

Die Anrufsignalisierung (H.225/Q.931) und -kontrolle (H.245) bei H.323 kann ebenfalls mittels TLS abgesichert werden. Dazu wird bei der Verwendung von TLS ein sicherer H.225-Kanal auf dem TCP-Port 1300 aufgebaut und darüber der Aufbau eines sicheren authentifizierten H.245-Kanals zwischen den Teilnehmern veranlasst [IT05a, Kap. 7].

Beim Einsatz des SCCP kann die Signalisierung zwischen Endgeräte und dem *Call-Manager* ebenso mit TLS verschlüsselt werden. *Secure* SCCP wird bei Cisco seit der Version 4 des *Call-Managers* unterstützt [Por06, S. 233].

S/MIME

Ein weiterer Sicherheitsmechanismus der innerhalb des SIP-Standards (RFC 3261[105]) spezifiziert wird, ist die Ende-zu-Ende-Verschlüsselung mittels S/MIME. Der Einsatz von S/MIME für den ganzen *Header* ist allerdings problematisch, da einzelne *Header-Felder* (*Request-URI, Route, Via und To*) der Pakete während des Transports zwischen den Teilnehmern von mehreren Netzkomponenten ausgewertet und verändert werden müssen [RSC+02]. Dies ist, sofern die an der Kommunikation beteiligten Netzkomponenten nicht das passende Schlüsselmaterial besitzen, nicht möglich.

Der SIP-Standard beschreibt zwei verschiedene Möglichkeiten, S/MIME einzusetzen. Im ersten Fall wird lediglich der *Body* verschlüsselt. Dadurch wird eine sichere Ende-zu-Ende Übertragung von Schlüsselmaterial mittels SDP möglich, wie es bei SRTP notwendig ist (siehe Kapitel 2.2.5). Anderenfalls kann die ganze SIP-Nachricht im *Body* mittels S/MIME geschützt und um einen *Header* im Klartext ergänzt werden, so dass dieser von beteiligten Netzkomponenten ausgewertet werden kann. Alle Implementierungen von S/MIME müssen mindestens den SHA-1-Algorithmus zur digitalen Signatur verwenden und *3DES* zur Verschlüsselung. Die Verwendung von *3DES* wurde jedoch durch RFC 3853 aufgehoben und der Einsatz von AES vorgeschrieben. Zur Bereitstellung des Schlüsselmaterials kommt bei S/MIME eine PKI zum Einsatz. Die Unterstützung von S/MIME ist im SIP-Standard allerdings optional gekennzeichnet und wird bisher von IP-Telefonen nicht unterstützt [Pet04].

IPSec

Unabhängig von den eingesetzten Protokollen lässt sich die Signalisierung mittels IPSec verschlüsseln. Im Umfeld von VoIP hat IPSec allerdings nur bei der Vernetzung von Gateways oder IP-Telefonanlagen über öffentliche Netzwerke praktische Relevanz. Eine Beschreibung des Protokolls IPSec erfolgt in Kapitel 2.2.8.

[105] [RSC+02]

M 8 Verschlüsselung der Sprachdaten

Um die Gespräche der Kommunikationspartner gegen Abhören und Manipulation zu schützen, muss die Übertragung der Sprachdaten verschlüsselt erfolgen. Diese Anforderung kann durch den Einsatz von IPSec und SRTP erfüllt werden. Dabei ist sicherzustellen, dass die Qualität der Sprachverbindungen bei aktivierter Verschlüsselung weiterhin den Anforderungen entspricht.

IPSec wird vorwiegend zur sicheren Vernetzung zweier Standorte über unsichere Netzwerke eingesetzt[106]. Dabei ermöglicht IPSec den Aufbau eines verschlüsselten Tunnels zwischen zwei vertrauenswürdigen Netzen auf der Vermittlungsschicht[107]. Somit kann jeglicher Datenverkehr unabhängig von dem verwendeten VoIP-Protokoll über den gesicherten Kanal ausgetauscht werden [KA98a, Kap. 3.1]. Der Einsatz von SRTP erfolgt sowohl zwischen IP-Telefonen als auch zur standortübergreifenden Absicherung zwischen IP-Telefonanlagen. Für die Verschlüsselung der Sprachdaten durch den Einsatz von SRTP, muss beim Transport des Schlüsselmaterials innerhalb der Signalisierung diese ebenfalls verschlüsselt werden. Andernfalls sind die in Kapitel 2.2.9 beschriebenen Protokolle zum Schlüsselmanagement einzusetzen, um einen sicheren Austausch des Schlüsselmaterials sicherzustellen. Die Funktionsweise und der Aufbau von SRTP und IPSec werden in Kapitel 2.2 beschrieben.

M 9 Absichern der Remote-Schnittstellen

Aktive Netzkomponenten werden im Allgemeinen über eine Remote-Schnittstelle, wie einem Web-Interface oder einer Remote-Konsole, verwaltet. Beim Einsatz von IP-Telefonen wird zusätzlich die Übertragung der Firmware und der Konfiguration durch Protokolle wie das TFTP oder das HTTP realisiert.

Grundlegend gilt, dass Remote-Schnittstellen deaktiviert sind, wenn sie nicht genutzt werden. Trifft das nicht zu ist es notwendig, dass der Zugriff auf die Schnittstellen mit Passwörtern gesichert ist und eine Übertragung der Daten nur über eine verschlüsselte Verbindung wie HTTPS oder Secure Shell (SSH) erfolgt. Als weiterer Sicherheitsmechanismus ist der Zugriff auf die Remote-Schnittstellen einzuschränken, so dass nur von ausgewählten Rechnern darauf zugegriffen werden kann. Sollte dies innerhalb der Konfigurationsmöglichkeiten der Endgeräte nicht möglich sein, kann der Zugriff durch eine geeignete Netzstruktur und den Einsatz von Firewalls eingeschränkt werden.

Beim Einsatz von Telnet und dem TFTP lassen sich Integrität, Vertraulichkeit und eine Authentifikation nicht sicherstellen. Ist deren Einsatz nicht vermeidbar, sind geeignete Maßnahmen zu ergreifen, welche die höchstmögliche Sicherheit für diese Protokolle ermöglichen. So kann die Integrität der auf TFTP-Servern

[106] Entsprechende Implementierungen in IP-Telefonen existieren zurzeit nicht.
[107] Schicht 3 des ISO/OSI-Referenzmodells

abgelegten Firmware und Konfigurationsdateien mit Hilfe von Host Intrusion Detection Systemen (HIDS) überwacht werden (siehe Maßnahme M 23 „Einsatz von IDS“). Wenn der Zugriff auf den TFTP-Server eingeschränkt wird und zusätzliche Maßnahmen gegen das Abhören der Kommunikationsverbindung umgesetzt werden, können mögliche Angriffspunkte minimiert werden.

M 10 Absichern der Multiportfunktion

Zahlreiche IP-Telefone besitzen einen dualen Ethernetanschluss, einen sogenannten Multiport. Dieser wird eingesetzt, wenn der Betrieb von IP-Telefonen aufgrund nicht ausreichend verfügbarer LAN-Dosen erschwert wird. Dazu besitzt das IP-Telefon zwei *Ethernetports* und ermöglicht so, dass ein Rechner direkt an das Endgerät angeschlossen werden kann und weitere Netzzugänge nicht benötigt werden.

Im Rahmen dieser Maßnahme ist sicherzustellen, dass die Multiportfunktion individuell abgesichert wird. Der Multiport muss deaktiviert sein, wenn er nicht genutzt wird [DIS06, Kap. 3.5.2.1]. Wird die Multiportfunktion eingesetzt, muss die in Maßnahme M 2 beschriebene Trennung von Sprach- und Datennetz durch den Einsatz von VLAN aufrecht erhalten werden [Hal03, S. 5]. Kommt im Netzwerk eine portbasierte Authentifizierung durch 802.1X zum Einsatz, ist die Konfiguration des Multiports entsprechend anzupassen (siehe Maßnahme M 15 „Sichere Endgeräteauthentifizierung mittels IEEE 802.1X“).

M 11 Sichere Konfiguration der IP-Telefone

Beim Einsatz von IP-Telefonen muss gewährleistet werden, dass diese ähnlich wie bei einem PC sicher konfiguriert eingesetzt werden. Somit ist sicherzustellen, dass die kritischen Leistungsmerkmale, wie zum Beispiel der *DTMF-Mode* über SIP, die Chefsekretärin-Funktion (*Intercom-Funktion*), die automatische Rufannahme (*Auto-Answer-Funktion*) oder die Rufumleitung vom Zieltelefon (*Follow-Me-Funktion*) deaktiviert sind und nach Bedarf individuell freigeschaltet werden.

Ebenfalls ist dafür Sorge zu tragen, dass mögliche Sicherheitseinstellungen im Telefon aktiviert werden. Dazu gehört der im Folgenden beschriebene Passwortschutz für die IP-Telefone. Dieser ist notwendig, da eine Konfiguration der Endgeräte auch direkt am Gerät möglich ist. So können beispielsweise die Zugangsdaten geändert und Netzwerk- und VLAN-Einstellungen vorgenommen werden. Eine solche Veränderung der Konfiguration durch den Anwender oder einen Angreifer stellt ein mögliches Sicherheitsrisiko dar. Folglich muss durch den Einsatz eines sicheren Passwortes verhindert werden, dass die Konfiguration von keinem Anwender ohne administrative Rechte geändert oder Sicherheitseinstellungen deaktiviert werden können.

Neben den bisherigen Sicherheitseinstellungen sind die IP-Telefone zusätzlich auf unsichere Standardeinstellungen zu überprüfen. Dies beinhaltet, dass bei der In-

betriebnahme der Geräte gewährleistet wird, dass herstellerabhängige voreingestellte Passwörter geändert werden. Dies ist notwendig, da die Passwörter in den zugehörigen Handbüchern und mitunter auch öffentlich dokumentiert werden und damit auch möglichen Angreifern bekannt sind.

Für den sicheren Betrieb der IP-Telefone müsse diese in einem privaten Adressbereich nach RFC 1918[108] betrieben werden. Bei einer ordnungsgemäßen Konfiguration von NAT ist gewährleistet, dass ein direkter Zugriff aus dem Internet auf das Sprachsegment nicht möglich ist [Hal03, S. 7].

Die Überprüfung der Endgerätekonfiguration erfordert eine genaue Kenntnis der einzelnen Konfigurationsparameter des eingesetzten Telefons. Gegebenenfalls existieren Dokumente, die eine sichere Konfiguration des IP-Telefons beschreiben. Zusätzlich ist durch eine regelmäßige Überprüfung sicherzustellen, dass die IP-Telefone den Anforderungen entsprechend konfiguriert sind.

M 12 Einsatz von Profilen für Endgeräte

Beim Einsatz der IP-Telefonie ist zu berücksichtigen, dass in einigen Fällen die IP-Telefone für jedermann zugänglich sind. Damit besteht die Gefahr, dass solche Geräte für den Gebührenbetrug benutzt werden (siehe Gefährdung G 7 „Gebührenbetrug“). So muss dem Telefon am Empfang (*Lobby*) ein Profil zugewiesen werden. Diese Zuordnung stellt sicher, dass nur eingeschränkte Leistungsmerkmale und Wahlmöglichkeiten, wie die Wahl einzelner fest definierter Rufnummern, zur Verfügung stehen. Weiterhin muss die Zuweisung von Profilen für alle Telefone umgesetzt werden, über die nur interne Gespräche geführt werden sollen oder Leistungsmerkmale wie die externe Rufweiterleitung nicht zur Verfügung stehen sollen.

M 13 Patchmanagement

Fehlendes oder unsicheres Patchmanagement kann eine zusätzliche Gefahrenquelle in VoIP-Netzwerken darstellen. Mögliche Gefährdungen, die durch Sicherheitslücken entstehen können, sind in Gefährdung G 5 „Ausnutzen von Implementierungsfehlern“ beschrieben. Das Patchmanagement soll sicherstellen, dass Sicherheitslücken zeitnah beseitigt werden, um so mögliche Angriffe, die ein System kompromittieren oder bei der Verarbeitung weiterer Anfragen einschränken, abzuwenden.

Maßnahmen der IT-Grundschutz-Kataloge[109] beschreiben in diesem Zusammenhang weitere Anforderungen an das Patchmanagement, die ebenfalls im Rahmen dieser Maßnahme umzusetzen sind. Diese betreffen zum einen die Vertraulichkeit

[108] [RMKGEL96]

[109] M 2.273 „Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates“ und M 4.83 „Update/Upgrade von Soft- und Hardware im Netzbereich“

der Patches, zum anderen wird eine vorige Evaluierung der Patches empfohlen. Weiterhin muss ein Patchvorgang dokumentiert werden und den Betreibern des Netzes Informationen zu Sicherheitslücken rechtzeitig bekannt sein, um diese zu beseitigen oder entsprechende Maßnahmen zur Absicherung umzusetzen [BSI05b, S. 875 ff, M 2.35].

M 14 Authentifizierung der Endgeräte

Bevor sich VoIP-Endgeräte bei einem angebotenen Dienst registrieren können, ist sicherzustellen, dass diese sich gegenüber Servern mindestens durch das Senden eines Passwortes[110] und Benutzernamens authentifizieren müssen. Wenn die Authentifizierung der Endgeräte nicht durch ein angemessenes Verfahren umgesetzt wird, kann eine sichere Nutzung der VoIP-Infrastruktur nicht sichergestellt werden.

Mögliche Verfahren werden abhängig von dem eingesetzten Signalisierungsprotokoll im zugehörigen Prüfkriterium P 11 genannt. Eine Authentifizierung der Endgeräte anhand ihrer MAC-Adresse ist kein angemessenes Verfahren zur Authentifizierung, da eine MAC-Adresse nicht fälschungssicher ist und somit durch einen Angreifer nachgeahmt werden kann [Hal03, S. 7].

Ferner ist die Vertraulichkeit der Authentifizierungsdaten sicherzustellen. So ist eine Authentifizierung durch Passwörter, welche im Klartext übertragen werden, ebenfalls kein angemessenes Verfahren.

Bei der Nutzung eines Mailbox-Dienstes ist der Zugang durch eine PIN zu schützen. Soll innerhalb der betreuten VoIP-Infrastruktur die Nicht-Abstreitbarkeit von Gesprächen sichergestellt werden, müssen sich Nutzer bei Gesprächen durch eine PIN gegenüber dem Telefon authentifizieren.

M 15 Sichere Endgeräteauthentifizierung mittels IEEE 802.1X

Um einen unautorisierten Zugriff von Endgeräten auf ein Netz wirkungsvoll einzuschränken, muss eine portbasierte Netzwerkzugangskontrolle durch IEEE 802.1X[111] zum Einsatz kommen. Der Zugang von Endgeräten lässt sich hierbei bereits am jeweiligen physikalischen Port kontrollieren.

Neben Mechanismen zur Schlüsselverwaltung stellt der IEEE-Standard 802.1X das Extensible Authentication Protocol (EAP) zum Austausch von Authentifizierungsdaten und zur Kontrolle des Zustands des *Supplicant*[112] bereit. Um die Authentifizierung auf Schicht 2 des ISO/OSI-Referenzmodells zu ermöglichen,

[110] Bei der Wahl des Passwortes muss sichergestellt werden, dass dieses eine hinreichende Komplexität besitzt (siehe Maßnahme M 2.11 „Regelung des Passwortgebrauchs“ [BSI05b, S. 845 ff, M 2.11]).

[111] [JCS04a]

[112] Als *Supplicant* wird ein Client bezeichnet der sich gegenüber dem *Authenticator*, wie einem Switch, authentifizieren möchte [JCS04a, Kap. 3.1.12].

werden die EAP-Pakete in *Ethernet-Frames* gekapselt (EAPOLAN). Die Authentifizierung erfordert einen Server, wie zum Beispiel einen RADIUS-Server, der die Überprüfung der Authentifizierungsdaten übernimmt und entscheidet, ob der Zugriff auf das Netz gewährt oder verweigert wird. Beim Einsatz eines RADIUS-Servers wird das EAP im RADIUS-Protokoll gekapselt[113], um eine Kommunikation zwischen *Supplicant* und dem Authentifizierungsserver zu ermöglichen. Das eigentlich genutzte Authentifizierungsverfahren wird mittels EAP-Methoden wie EAP-TLS, EAP-PEAP, EAP-TTLS und EAP-MD5 bereitgestellt [HWPT05; AAG+05; JCS04a].

Zudem werden Mechanismen zum Management bereitgestellt, mit denen abhängig von der Authentifizierung einem Port eine VLAN-ID zugewiesen werden kann. Somit ist es möglich, ein VLAN einzurichten, in dem sich Objekte mit fehlerhafter Authentifizierung befinden, die jedoch ebenfalls per DHCP eine IP-Adresse bekommen und so gegenüber dem Management weiter erreichbar sind [JCS04a, Kap. C.2.1].

Bei VoIP-Endgeräten, die eine Multiportfunktion besitzen ist im Zusammenhang mit IEEE 802.1X zu berücksichtigen, dass eine Authentifizierung unabhängig vom Zustand der Authentifikation des Computers oder des IP-Telefons möglich ist. Das bedeutet, dass ein Computer sich authentifizieren kann, auch wenn das IP-Telefon sich noch nicht erfolgreich registriert hat oder gerade neu bootet. Kann sich ein Computer unabhängig vom Zustand des IP-Telefons authentifizieren, ist darauf zu achten, dass bei der Aktivierung von IEEE 802.1X eine *Multi-Host-Option* die zusätzliche Authentifizierung des IP-Telefons zulässt [Jam02, S. 10].

M 16 Absicherung der Netzübergänge zu öffentlichen VoIP-Netzwerken

Wird die IP-Telefonie über eine reine VoIP-Infrastruktur realisiert, muss das interne Netzwerk gegenüber Angriffen aus dem öffentlichen VoIP-Netzwerk geschützt werden. Der Einsatz von Firewalls oder auch Session Border Controller (SBC) stellt sicher, dass netzübergreifende Angriffe, wie sie von externen Angreifern ausgehen, unterbunden werden[114].

Die im folgenden beschriebenen Komponenten Firewall und SBC stellen beim Einsatz einen *Single Point of Failure* dar und müssen somit im Rahmen der Maßnahme M 1 „Redundante Auslegung wichtiger Netzkomponenten“ berücksichtigt werden. Weiterhin verursachen beide Komponenten häufig einen Bruch bei der Umsetzung einer Ende-zu-Ende-Verschlüsselung. Dies resultiert aus der notwendigen Analyse der Pakete zur Sicherstellung ihrer Funktionalität. Aufgrund ihrer zentralen Position in Netzwerken, ist ebenfalls auf eine Unterstützung von QoS-Mechanismen und eine ausreichende Dimensionierung der benö-

[113] RFC 3579 [AC03]

[114] Eine Übersicht über netzwerkbasierte und protokollspezifische Angriffe ist im Kapitel A.3 zu finden.

tigten Rechenkapazität zu achten, damit sie nicht die Ursache für Paketverluste oder Verzögerungen sind. Die Umsetzung der ALG-Funktionalität erfordert zudem, dass Erweiterungen der VoIP-Protokolle zeitnah vom Hersteller umgesetzt werden [JP06, S.90 ff.].

Firewalls

Mit Hilfe von Firewalls können Sicherheitsrichtlinien an zentraler Stelle umgesetzt werden. Zudem bieten sie die Möglichkeit, unautorisierten ausgehenden und ankommenden Verkehr zu unterbinden sowie eine Protokollierung abgelehnter oder zugelassener Verbindungen durchzuführen. Da Firewalls anhand zahlreicher Regeln detailliert konfiguriert werden können, stellen sie mit der Kontrolle von Netzübergängen einen wesentlichen Mechanismus zur Strukturierung von Netzwerken bereit. Sie bieten zusätzlich die Möglichkeit NAT durchzuführen und somit mehreren Nutzern eine öffentliche IP-Adresse zur Verfügung zu stellen. Gleichzeitig wird die interne Architektur gegenüber dem öffentlichen Netz verborgen.

Der Einsatz einer Firewall und NAT in einer VoIP-Infrastruktur erfordert zusätzlich ein ALG. Dieses ist für die Funktionalität der Firewall notwendig, da innerhalb der Signalisierung bei Protokollen wie SIP und H.323 die für die Übertragung der Sprachdaten verwendeten Ports dynamisch zwischen den Kommunikationspartnern vereinbart werden. Bei der Umsetzung der NAT-Funktionalität ist ein ALG erforderlich, da ein Umschreiben der Adressen (IP-Adresse und Port) innerhalb der Signalisierung nicht vorgesehen ist. Die Ursache dafür ist, dass eine Firewall beziehungsweise ein NAT-Gateway nur auf den ISO/OSI-Schichten 3 und 4 arbeitet und somit übermittelte Adressen auf höheren Schichten nicht interpretiert (Firewall) beziehungsweise umgeschrieben (NAT-Gateway) werden können. Der Einsatz eines ALG ermöglicht dagegen, den Datenverkehr auf Applikationsebene zu analysieren und die Vereinbarung der Adressen zwischen den Kommunizierenden im jeweiligen Protokoll zu erkennen. Somit können Ports dynamisch geöffnet (Firewall) oder die Adressen entsprechend umgeschrieben (NAT-Gateway) werden. Die beschriebene Funktionalität bezüglich der Interpretation von VoIP-Protokollen wird in der Fachterminologie als *VoIP-aware* bezeichnet. Aufgrund der aufwendigen Analyse der Pakete durch ein ALG ist die Aufrechterhaltung der Dienstgüte unter hoher Last sicherzustellen [AAG+05; TW05].

SBC

Eine Kombination aus Firewall-, ALG- und Proxy-Funktionalität bieten Session Border Controller (SBC). Sie werden häufig bei Internet-Service-Providern (ISP) eingesetzt, die damit den gesetzlichen Anforderungen sowie denen an Verfügbarkeit und Sicherheit ihrer Netze gerecht werden wollen. Ein SBC bietet gegenüber der internen VoIP-Infrastruktur eine sichere Terminierung der VoIP-Verbindungen, so dass protokollspezifische Angriffe die VoIP-Endgeräte nicht erreichen. Die Terminierung wird erzielt, indem protokollabhängig Proxys als Vermittlungssystem betrieben und somit Pakete nicht weitergeleitet sondern neu

generiert werden. Dies ermöglicht zusätzlich, die Topologie und die IP-Adressen gegenüber dem externen Netz zu verbergen, indem interne IP-Adressen in VoIP-Paketen nicht nach außen weitergeben werden. So werden bei SIP IP-Adressen im *Header-Feld VIA*[115], die einen Rückschluss auf die interne Topologie ermöglichen, entfernt.

Zusätzlich bieten SBC die Möglichkeit der Umsetzung von *Traffic*- und Bandbreitenmanagement, die Weiterleitung und Zusammenführung von verschiedenen Sprachprotokollen, die Rufannahmesteuerung, die Abrechnung sowie die Einrichtung von gesetzlichen Abhörstationen [JP06; AAG+05].

M 17 Absichern der IP-Telefonanlage

Das gezielte systemspezifische Absichern von Servern wird auch als „Härten“ bezeichnet. Angesichts der in Gefährdung G 5 „Ausnutzen von Implementierungsfehlern“ beschriebenen Möglichkeiten der Kompromittierung, muss das Härten auch für eine IP-Telefonanlage umgesetzt werden. Dabei werden mögliche Angriffspunkte auf das darunter liegende Betriebssystem eingeschränkt, indem netzwerk- und systemspezifische Schwachstellen beseitigt und zusätzliche Sicherheitsmechanismen ergriffen werden. Im Folgenden sind einige Kriterien gegeben, die bei der Härtung eines Servers berücksichtigt werden sollten [JP06; Por06].

- Deaktivieren und Deinstallieren von nicht benötigten Diensten.
- Einschränken von Rechten, mit denen Dienste ausgeführt werden
- Einsatz einer Firewall[116]
- Überprüfen und Anpassen von Standardeinstellungen[117]
- Überprüfen der angelegten Benutzerkonten und deren Berechtigungen
- Deaktivieren nicht verwendeter und kritischer Leistungsmerkmale
- Schutz von sensiblen TK-Daten (Zugangsdaten, Verbindungsnachweise)
- Einführung von HIDS auf gehärteten Servern[118]

Das BSI stellt in den IT-Grundschutz-Katalogen[119] zusätzliche Maßnahmen für die Absicherung von einzelnen Betriebssystemen wie Windows und Linux zur

[115] siehe Tabelle 1 im Kapitel 2.2.1
[116] Anforderungen an Firewalls sind in Maßnahme M 16 „Absicherung der Netzübergänge zu öffentlichen VoIP-Netzwerken“ beschrieben.
[117] Dies gilt besonders für herstellerspezifische Standardpasswörter.
[118] siehe Maßnahme M 23 „Einsatz von IDS“
[119] [BSI05b]

Verfügung. Diese sollten beim jeweiligen Betriebssystem angewendet werden. Gegebenenfalls existieren vom Hersteller spezielle Dokumente, die zur Absicherung des Systems herangezogen werden können.

M 18 Absichern der Basis-Netzwerkdienste

Mit Umsetzung dieser Maßnahme sollen grundlegende Angriffe auf die Basis-Netzwerkdienste ARP und DHCP unterbunden werden. Aufgrund der Übertragung der Sprache über das Internetprotokoll ist VoIP ebenso anfällig auf Angriffe innerhalb der ISO/OSI-Schichten 2 und 3, wie das in bisherigen Datennetzen der Fall ist. Dazu gehören in erster Linie Angriffe, die das Abhören ermöglichen oder die Verfügbarkeit einschränken.

ARP

Eine feste Zuordnung der Ports und MAC-Adressen am Switch bietet die Möglichkeit eine Manipulation der Zuordnungstabelle durch *MAC-Spoofing-Angriffe* zu vermeiden. Dieser Mechanismus kann allerdings in größeren Netzen administrativ nicht umgesetzt werden und ist somit nicht zu empfehlen. Die BSI-Studie VoIPSEC rät in diesem Zusammenhang, dass „*für alle kritischen Systeme wie VoIP-Server, Gateways und Gatekeeper [...] feste MAC-Zuordnungen vorgenommen werden [sollten]*“ [AAG+05, S. 75].

Häufig unterstützt bereits ein Switch einen Mechanismus, der die Kontrolle der ARP-Nachrichten vornehmen kann und somit eine Manipulation des *ARP-Caches* (*ARP-Spoofing*) nicht möglich ist, wie beispielsweise Dynamic ARP Inspection (DAI) bei Komponenten der Firma „Cisco“. Durch die Begrenzung der Anzahl von ARP-Paketen besteht zudem die Möglichkeit, die Überflutung eines Switches mit ARP-Nachrichten (*MAC-Flooding*) abzuwehren [Cis, S. 39-1].

Um Unregelmäßigkeiten bei der Zuordnung von MAC- zu IP-Adressen im Netzwerk erkennen zu können, existieren Programme wie *Arpwatch* oder spezielle Produkte wie *ARP-Guard*, die ebenfalls die Auffälligkeiten entsprechend protokollieren und benachrichtigen. Solche Produkte müssen dabei keinesfalls überall integriert werden, sondern lediglich an zentralen Netzknoten wie Routern, die bei einer Trennung von Server- und Client-Systemen[120] in jedem Fall Ziel eines solchen Angriffs sind.

DHCP

Für die Zuweisung der Netzwerkparameter bei VoIP-Endgeräten kommt das DHCP zum Einsatz. Den Endgeräten werden beim Booten Parameter wie IP-Adresse, Gateway, DNS-Server und NTP-Server zugewiesen. Herstellerabhängig wird ein Server für die *Firmware* und die Konfigurationsdatei für die VoIP-Umgebung bestimmt. Aufgrund der mangelnden Authentizität und Integrität der

[120] Die in Maßnahme M 2 „Trennung von Sprach- und Datennetz“ beschriebene Trennung von Endgeräten kann auch auf Server- und Client-Systeme angewendet werden.

Parameter ist das DHCP häufig ein erster Ansatzpunkt, um einen Angriff vorzubereiten. Angriffe auf einen DHCP-Server können die Verfügbarkeit des DHCP-Dienstes einschränken[121] oder die Konfiguration der Endgeräte beeinflussen[122] [DA01, Kap. 1].

Ähnlich wie DAI bei gefälschten ARP-Nachrichten können beim DHCP mit herstellerspezifischen Lösungen, wie Cisco's *DHCP-Snooping*, gefälschte Nachrichten erkannt und eine Weiterleitung verhindert werden. Wird die Anzahl der DHCP-Anfragen pro Sekunde eingeschränkt, können bei einem DoS-Angriff auf den DHCP-Server, die Anfragen an diesem Port unterdrückt werden [Cis, 38-2].

M 19 USV für die Middleware

Eine USV-Anlage[123] ermöglicht die Überbrückung von kurzzeitigen Stromausfällen für die Middleware[124]. Dadurch können bei einem Stromausfall die Komponenten geregelt heruntergefahren werden, um Schäden wie einen Datenverlust zu vermeiden. In Verbindung mit PoE ermöglicht eine USV-Anlage auch die Versorgung der Endgeräte (siehe Maßnahme M 20 „USV für IP-Telefone").

Bei der Dimensionierung einer USV-Anlage geben die IT-Grundschutz-Kataloge eine Hilfestellung. So wird in der Maßnahme M 1.28 „Lokale unterbrechungsfreie Stromversorgung" die von einer USV-Anlage zu überbrückende Zeit auf 10 bis 15 Minuten beziffert. Diese Angabe beruht auf Erfahrungen, nach denen ein Stromausfall in der Regel nach 5-10 Minuten behoben ist. Zudem wird in der Maßnahme darauf hingewiesen, dass die Schutzwirkung der USV-Anlage durch regelmäßige Wartungen sichergestellt werden muss [BSI05b, S. 764 ff.].

Zusätzlich können erhöhte Anforderungen an die Verfügbarkeit verlangen, dass die Aufrechterhaltung des Betriebes für eine definierte Zeitspanne sichergestellt werden muss. In diesem Fall werden zusätzliche Maßnahmen wie der Einsatz von Dieselgeneratoren oder einer Netzersatzanlage[125] erforderlich [AAG+05, S. 73].

M 20 USV für IP-Telefone

Um das Telefonieren bei kurzzeitigen Stromausfällen zu ermöglichen, ist neben der unterbrechungsfreien Stromversorgung der Middleware, diese auch für die IP-Telefone durch den Einsatz von Power over Ethernet (PoE) sicherzustellen.

PoE wird im IEEE-Standard 802.3af[126] standardisiert und ermöglicht es Endge-

[121] Ein Beispiel dafür ist ein sogenannter DHCP-Starvation-Angriff, bei dem alle verfügbaren DHCP-Adressen an den Angreifer gebunden werden, in dem dieser stetig mit veränderter MAC-Adresse neue Anfragen an den DHCP-Server stellt [AAG+05, S. 52].

[122] Dies wird durch das Platzieren von fremden Servern (engl. *rogue devices*) realisiert, die sich gegenüber den Endgeräten als Server ausgeben und somit versuchen die Nachrichten für ihre Zwecke wie einen MitM-Angriff zu manipulieren [DA01, Kap. 1.1].

[123] Unterbrechungsfreie Stromversorgung (USV)

[124] IP-PBX, Switches und Router und Basis-Netzwerkdienste

[125] siehe M 1.56 „Sekundär-Energieversorgung" [AAG+05, S. 800 ff.]

[126] [GLW+05]

räte wie IP-Telefone über das *Ethernet-Kabel* mit Strom zu versorgen. Somit benötigen die IP-Telefone kein extra Netzteil, um die Stromversorgung des Gerätes sicherzustellen. Sie können über das Ethernet-Kabel auf eine Entnahmeleistung von 12,95 Watt zurückgreifen. Für die Speisung der Ethernet-Kabel ist das sogenannte Power Source Equipment (PSE) zuständig, das die Versorgung der Endgeräte, den sogenannten Power Devices (PD), übernimmt [GLW+05; AAG+05].

Für die Platzierung des PSE werden im IEEE-Standard 802.3af zwei verschiedene Varianten genannt. Zum einen gibt es die Möglichkeit das PSE im Switch zu integrieren (Endpoint) und zum anderen als extra Komponente, welche die Speisung der Switches übernimmt (Midspan). Bei Verwendung von Midspan-Systemen lässt sich, in Verbindung mit einer USV-Anlage an zentraler Stelle, die unterbrechungsfreie Stromversorgung aller über PoE angeschlossenen Geräte sicherstellen. Zudem erlauben Midspan-Systeme eine nachträgliche Integration in ein bestehendes Netz. Nachteilig bei diesen Systemen ist, dass in jedem Fall zwei Adernpaare benötigt werden und somit bei angewendetem *Cable Sharing* eine Integration nicht möglich ist [GLW+05; AAG+05].

M 21 Physische Zutrittskontrolle

VoIP- und Netzkomponenten sind ebenso in abgesicherten Räumen unterzubringen, wie die bisherigen System- und Netzkomponenten im Datennetz. Zutritt zu diesen Räumlichkeiten darf nur autorisiertem Personal möglich sein. Diese notwendige Zutrittskontrolle kann je nach verfügbarem Budget der Firma und entsprechendem Schutzbedarf variieren. Anforderungen an eine Zutrittsregelung und -kontrolle werden von den IT-Grundschutz-Katalogen in Maßnahme M 2.17 „Zutrittsregelung und -kontrolle“ formuliert und sind ebenso auf VoIP-Infrastrukturen anzuwenden [BSI05b, S. 852 ff.]:

- „*der von der Regelung betroffene Bereich [muss] eindeutig bestimmt [werden] [...]*“
- „*die Zahl der zutrittsberechtigten Personen [muss] auf ein Mindestmaß reduziert [werden] [...]; diese Personen sollen gegenseitig ihre Berechtigung kennen, um Unberechtigte als solche erkennen zu können.*“
- „*der Zutritt anderer Personen (Besucher) [darf] erst nach vorheriger Prüfung der Notwendigkeit [erfolgen] [...]*“
- „*erteilte Zutrittsberechtigungen [müssen] dokumentiert werden*“

Eine geeignete Zutrittskontrolle stellt nach wie vor das Abschließen der abgesicherten Räume dar. Dieses erfordert jedoch zusätzliche Maßnahmen zur Schlüsselverwaltung, um einen ausreichenden Schutz zu bieten (siehe „M 2.14 Schlüsselverwaltung“ [BSI05b, S. 349]). Zusätzliche Möglichkeiten der Zutrittskontrolle bieten

die Verwendung von *Smartcards* oder biometrischen Merkmalen, die zudem eine Protokollierung und Personenvereinzelung erlauben. Die alleinige Verwendung von biometrischen Verfahren zur Zutrittskontrolle ist jedoch „*aus heutiger Sicht [...] als alleinige Zutrittskontrolle nicht zu empfehlen*“ [BSI05b, S. 853, M 2.17].

M 22 Sicherstellen der Notrufmöglichkeit

Aufgrund der in Gefährdung G 15 „Fehlende oder eingeschränkte Notrufmöglichkeit“ beschriebenen unzureichenden Umsetzung der Notrufanforderungen, muss eine Notrufmöglichkeit durch eine der folgenden Maßnahmen bereitgestellt werden.

Zum einen kann die Notruffunktionalität durch einen TK-Basisanschluss sichergestellt werden. Damit diese beim Ausfall der IP-Telefonanlage weiterhin zur Verfügung steht, muss an einem separaten TK-Basisanschluss ein Notruftelefon bereitgestellt werden [BSI05b, S. 2936, M 6.29]. Folglich muss sowohl bei reiner IP-Telefonie als auch bei einer bereits existierenden Außenanbindung an das Festnetz ein Notruftelefon direkt am Amtsanschluss zur Verfügung stehen.

Eine Alternative, die Notrufmöglichkeit unabhängig von der IP-Telefonanlage bereitzustellen, bietet die Nutzung eines Mobiltelefons [TAO06a, S. 39]. Aufgrund der großen Verbreitung von Mobiltelefonen und der umgesetzten Ortsbestimmung bei mobiler Nutzung stellt dies eine praktikable Alternative dar. Bei dieser Möglichkeit existieren zudem keine weiteren Kosten, da die Notrufmöglichkeit auch ohne gültigen Mobilfunkvertrag verfügbar ist.

M 23 Einsatz von IDS

Intrusion Detection Systeme (IDS) bieten, wenn sie richtig eingesetzt werden, eine sinnvolle Ergänzung zur Sicherheit in Netzwerken. Dabei wird zwischen den beiden Varianten Network Intrusion Detection System (NIDS) und Host Intrusion Detection System (HIDS) unterschieden. Beide IDS-Varianten können parallel eingesetzt werden, um Angriffe im Netzwerk (NIDS) und Anomalien bei den Netzkomponenten selbst (HIDS) zu erkennen. Auf die Funktionsweise und deren sinnvollen Einsatz soll im Folgenden eingegangen werden.

Ein NIDS besteht im allgemeinen aus mehreren Sensoren, die im Netzwerk verteilt sind und anhand von verfügbaren Signaturen Auffälligkeiten im Netzwerkverkehr erkennen. Solche Auffälligkeiten können zum Beispiel gezielte Angriffe (z.B. *Exploits*) oder Unregelmäßigkeiten im Netzwerkverkehr (z.B. *Portscans*) sein. Im weiteren werden diese Auffälligkeiten von den Sensoren an eine zentrale Instanz übermittelt und protokolliert. Zusätzlich zu dieser Echtzeitüberwachung erlauben es NIDS, gezielt auf Anomalien zu reagieren und Gegenmaßnahmen einzuleiten. So kann der Netzwerkverkehr des Verursachers blockiert oder gezielt eine TCP-Verbindung durch ein Reset unterbrochen werden [Hal03].

Bei der Platzierung der Sensoren ist darauf zu achten, dass diese möglichst zentral positioniert sind und zudem mögliche Gefahrensituationen abdecken. Demnach ist der Einsatz von Sensoren an einem vermittelnden Knotenpunkt zwischen Daten-, Server- und VoIP-Segment und ebenfalls beim Übergang zu einer DMZ[127] sinnvoll [Por06].

Ein HIDS bietet die Möglichkeit, Informationen zu Veränderungen am Dateisystem eines Servers bereitzustellen. Zudem können Protokolldateien sowie das Betriebssystem auf Auffälligkeiten untersucht werden. Bevor ein solches System zum Einsatz kommen kann, ist vor der Konfiguration des einzelnen Systems die Maßnahme M 17 „Absichern der IP-Telefonanlage“ durchzuführen.

M 24 Maßnahmen gegen automatisierte unerwünschte Werbeanrufe

In der Beschreibung der Gefährdung G 14 „Unerwünschte Werbeanrufe“ wurde bereits auf die aktuell geringe Bedeutung von SPIT eingegangen. Aus diesem Grund existieren bisher nur Konzepte und Prototypen zur Bekämpfung von SPIT, die sich im täglichen Einsatz mit realem SPIT erst noch bewähren müssen. Dennoch soll in dieser Maßnahme auf Möglichkeiten der Erkennung und Behandlung von SPIT eingegangen werden, da mit einer zunehmenden Ende-zu-Ende-Kommunikation über VoIP die Gefährdung durch SPIT zunehmen wird und somit existierende Konzepte in VoIP-Lösungen zu integrieren sind.

Der Kieler Internet Provider „TNG - THE NET GENERATION AG“ und das „Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein“ haben innerhalb des Projektes „SPIT-AL“ eine rechtskonforme Lösung für einen SPIT-Filter ausgearbeitet.

„*Kernstück der Lösung sind White- und Blacklists in einer verteilten Realisierung, anhand derer die Anruferkennungen klassifiziert werden. Zusammen mit weiteren Informationen, zum Beispiel statistischen Bewertungen, ergibt sich daraus, wie der Anruf zu behandeln ist*“ [RTH+06, S. 3].

Dabei nimmt der *Application-Softswitch* den Anruf stellvertretend für den Anrufer entgegen. Anhand der verfügbaren Metadaten erfolgt eine Bewertung durch den Management-Server. Anschließend wird durch den *Application-Softswitch* die Umsetzung einer der im Folgenden genannten Maßnahmen veranlasst. Diese können beinhalten, dass ein Anruf vollständig oder temporär abgelehnt, angenommen oder auf eine Festnetznummer, eine Mailbox beziehungsweise ein Sprachmenü umgeleitet wird.

Bei der Bewertung der Metadaten durch den Management-Server setzt das „SPIT-AL-Projekt“ ähnlich heutiger SPAM-Mechanismen auf ein Bewertungssystem anhand von Punkten. Die Bewertungskriterien für die Vergabe der Punkte sind dabei die Herkunft eines Anrufes, private und importierte *White-* sowie *Blacklisten.*

[127] Demilitarisierte Zone (DMZ)

Private *Black*- und *Whitelisten* können dabei durch den jeweiligen Nutzer über ein Web-Interface verwaltet, gegebenenfalls veröffentlicht oder als veröffentlichte Liste in die Bewertung einbezogen werden. Zudem können statische Blacklisten genutzt werden, die insbesondere für VoIP-Service-Provider wertvoll bei der Erkennung von SPIT-Anrufen aus dem eigenen Netzwerk sind [RTH+06].

Bereits zum jetzigen Zeitpunkt können automatisierte Anrufe erfolgreich abgewehrt werden, indem Gespräche über ein Sprachmenü geleitet werden und nur über die Nutzung der Tonwahl die Vermittlung zum gewünschten Gesprächspartner ermöglicht wird.

6 Prüfkriterien

6.1 Prüfkriterienübersicht

6.2 Prüfkriterien

P 1 Redundante Auslegung wichtiger Netzkomponenten

Das Kriterium ist erfüllt, wenn ein den Anforderungen an Verfügbarkeit angemessenes Redundanzkonzept umgesetzt wurde und anhand der folgenden Kriterien geprüft würde.

- Spiegelt das Redundanzkonzept die für das VoIP-Netzwerk definierten Verfügbarkeitsanforderungen wieder?
  - Wird eine Unterbrechung der Telefongespräche oder ein nicht möglicher neuer Aufbau von Gesprächen toleriert?
  - Erfolgt eine automatische Funktionsübernahme der redundanten Komponenten?
- Existieren *Single Points of Failure* im Netzwerk?
  - IP-PBX, Router, Switch, DHCP-Server, Firewall, SBC, USV-Anlage und Verkabelung

P 2 Trennung von Sprach- und Datennetz

Das Kriterium ist erfüllt, wenn eine logische Trennung durch VLAN oder eine physikalische Trennung für Endgeräte aus dem Sprach- und Datennetz erfolgt. Die Umsetzung der Segmentierung ist dabei anhand der folgenden Kriterien positiv zu prüfen.

Prüfung der logischen Trennung

- Sprach- und Datennetz werden in zwei unterschiedlichen privaten Adressbereichen betrieben.
- Der Zugriff zwischen den VLANs ist nicht möglich. Werden Dienste netzübergreifend genutzt, muss eine Firewall die Kommunikation auf die zum Betrieb der Dienste notwendigen Daten einschränken.
- Die Anzahl der Endgeräte pro Broadcastdomäne ist angemessen.
- Nicht verwendete Ports des VLAN-Switches sind deaktiviert oder erhalten eine unbenutzte VLAN-ID [BR06], sofern der VLAN-Switch nicht vor unbefugtem Zutritt geschützt ist.

- Das *VLAN-Trunking* ist nur an Ports gestattet, an denen sich autorisierte Switches oder IP-Telefone mit Multiport befinden [BR06].
- Es ist sichergestellt, dass durch den Missbrauch von *Trunking-Protokollen* kein Zugriff auf alle VLANs möglich ist.

Prüfung der physikalischen Trennung

- Sprach- und Datennetz werden in zwei unterschiedlichen privaten Adressbereichen betrieben.
- Der Zugriff zwischen den Netzen ist nicht möglich. Werden Dienste netzübergreifend genutzt, muss eine Firewall die Kommunikation auf die zum Betrieb der Dienste notwendigen Daten einschränken.
- Die Anzahl der Endgeräte pro Broadcastdomäne ist angemessen.

P 3 Sicherer Einsatz von Softphones

Das Kriterium ist erfüllt, wenn die Prüfung bezüglich der sicheren Integration von Softphones anhand der folgenden Anforderungen positiv abgeschlossen wird und zusätzlich das Prüfkriterium P 11 „Sichere Konfiguration der IP-Telefone“ ebenfalls auf Softphones angewendet wird.

- Die Zugangsdaten müssen verschlüsselt im Betriebssystem abgelegt werden.
- Der Zugriff auf die Anruflisten darf nur innerhalb der Software möglich sein.
- Die Software muss frei von *Adware* und *Spyware* sein.
- Der Betrieb der Software muss ohne administrative Rechte möglich sein.
- Beim Einsatz des IEEE-Standards 802.1X muss die Software diesen ebenfalls unterstützen.
- Die Software muss beim Einsatz von redundanten Servern, *Fail-Over-Mechanismen* wie *DNS SRV Ressource Records* bei SIP-Servern (RFC 2543) unterstützen.
- Der Zugriff von Softphones auf weitere Endgeräte muss auf die zur Funktion notwendigen Dienste eingeschränkt sein.

P 4 Kein Einsatz von Softphones

Das Kriterium ist erfüllt, wenn sichergestellt ist, dass installierte Softphones sich nicht zu Servern im Netzwerk und außerhalb des betreuten Netzwerkes verbinden können.

P 5 Bandbreitenmanagement

Das Kriterium ist erfüllt, wenn eine Bandbreitenplanung bei der Integration der IP-Telefonie gemacht wurde und eine der folgenden Architekturen gemäß den Anforderungen an die Dienstgüte umgesetzt wird. Ferner muss die IP-Telefonanlage die Anzahl der Verbindungen überwachen und regulieren.

Architekturen	CoS / QoS	geeigneter Einsatz
DiffServ	CoS	geroutete leistungsfähige Netzwerke[a]
IEEE 802.1 Q/p	CoS	private und Einzelsegment-Netzwerke
IntServ (RSVP)	QoS	geroutete Netzwerke mit limitierter Bandbreite[b]
MPLS	QoS	Provider-, große Enterprise- und ATM-Netzwerke
Overprovisioning	QoS	geeignet für Netzwerke jeder Art

Tabelle 16: QoS-Maßnahmen [Wal05]

[a] DiffServ ist nicht geeignet, wenn in einem Netzwerk mehr Sprache als Daten übertragen werden.

[b] IntServ ist nicht geeignet, wenn in einem Netzwerk mehr Daten als Sprache übertragen werden.

P 6 Monitoring und Logging

Das Kriterium ist zum einen erfüllt, wenn die folgenden Ereignisse protokolliert werden und die Anforderungen positiv für die Logging- und Monitoring-Architektur geprüft wurden.

Ereignisse

- Server
  - Auslastunsmerkmale der IP-PBX
  - Authentifizierung der VoIP-Endgeräte
  - Stromausfall
  - Sicherheitskritische Fehlermeldungen der Serverdienste

- Router und Switches
  - Fremdgeräte befinden sich im Netzwerk
  - Angriffe (z.B. DoS)
- IP-Telefone
  - IP-Telefonanlage nicht erreichbar
  - Basis-Netzwerkdienste nicht erreichbar
- alle Komponenten
  - Sowohl erfolglose als auch erfolgreiche Login-Versuche

Anforderungen

- Die zentrale Protokollierung ist auf allen Geräten aktiviert.
- Alle Logdaten werden regelmäßig ausgewertet.
- Bei system- und sicherheitskritischen Ereignissen erfolgt eine Benachrichtigung.
- Die Integrität und Authentizität der übertragenen sowie gespeicherten Daten ist sichergestellt[128].
- Die zeitliche Ordnung der protokollierten Daten ist sichergestellt.
- Eine Archivierung ermöglicht den Zugriff auf Logdaten zu einem späteren Zeitpunkt.

P 7 Verschlüsselung der Signalisierung

Das Kriterium ist erfüllt, wenn die Signalisierung im LAN zwischen Gateway und Endgerät, standortübergreifend zwischen Gateways oder zwischen Endgeräten mit TLS, S/MIME oder IPSec abgesichert ist.

[128] SNMPv3, Syslog über TCP (syslog-ng) und SSH

Die korrekte Umsetzung der Verschlüsselungsverfahren kann anhand der folgenden Bedingungen geprüft werden.

- Der Austausch der Signalisierungsnachrichten erfolgt verschlüsselt.
- Für die Kommunikationspartner ist zu erkennen, wenn die Signalisierung nicht verschlüsselt erfolgt.
- Beim Einsatz einer *Hop-by-Hop-Verschlüsselung* sind die an der Kommunikation beteiligten Netzknoten als vertrauenswürdig eingestuft.
- Beim Einsatz von Zertifikaten ist eine sichere Verteilung sichergestellt.

P 8 Verschlüsselung der Sprachdaten

Das Kriterium ist erfüllt, wenn Verfahren von beiden Kommunikationspartnern eingesetzt werden, die eine Verschlüsselung der Sprachdaten sicherstellen. Die Bedingungen für den Einsatz sollen im Folgenden die Prüfung ermöglichen.

- Der Austausch der Sprachdaten erfolgt verschlüsselt.
- Der Schlüsselaustausch bei SRTP wird zusätzlich abgesichert.
- Für die Kommunikationspartner ist zu erkennen, wenn keine Verschlüsselung über SRTP erfolgt oder wenn von einem verschlüsselten Transport der Sprachdaten auf einen unverschlüsselten gewechselt wird.
- Die Anzahl der maximalen Verbindungen kann bei zusätzlicher Verschlüsselung der Sprachdaten aufrecht erhalten werden.

P 9 Absichern der Remote-Schnittstellen

Das Kriterium ist erfüllt, wenn die folgenden Anforderungen beim Einsatz von Remote-Schnittstellen umgesetzt werden.

- Remote-Schnittstellen sind deaktiviert, wenn sie nicht genutzt werden.
- Die Administration der Netzkomponenten erfolgt verschlüsselt durch Protokolle wie HTTPS oder SSH.
- Der Zugriff auf die Remote-Schnittstellen ist durch ein Passwort geschützt.
- Der Zugriff auf die Remote-Schnittstellen ist auf IP-Adressen von ausgewählten Management-Stationen beschränkt.

- Der Zugriff auf die Konfigurationsdateien der IP-Telefone ist auf die aktiven Geräte eingeschränkt.
- Die Integrität und Vertraulichkeit der Konfigurationsdateien wird durch eine verschlüsselte Übertragung sichergestellt. Alternativ müssen Maßnahmen umgesetzt werden, die ein Abhören der Datenübertragung erschweren.

P 10 Absichern der Multiportfunktion

Das Kriterium ist erfüllt, wenn die folgenden Anforderungen für die Konfiguration der Multiportfunktion am IP-Telefon erfolgreich stichprobenartig geprüft wurden.

- Bei nicht genutzter Multiportfunktion muss der Multiport deaktiviert sein.
- Der Multiport kann nur durch Benutzer mit administrativen Rechten aktiviert werden.
- Bei der Nutzung der Multiportfunktion wird sichergestellt, dass ein IP-Telefon und ein angeschlossener Computer sich in dem zugehörigen Netzsegment befindet.

P 11 Sichere Konfiguration der IP-Telefone

Das Kriterium ist erfüllt, wenn die folgenden Kriterien exemplarisch für einige Endgeräte unter zu Hilfenahme der jeweiligen Dokumentation positiv geprüft wurden.

- Kritische Leistungsmerkmale wie *DTMF-Mode* über SIP, die *Intercom-Funktion*, die *Auto-Answer-Funktion* oder eine Rufumleitung wie die *Follow-Me-Funktion* sind per Default deaktiviert und können nur von autorisierten Personen aktiviert werden.
- Im Netzwerk werden keine Geräte mit schwachen oder Standardpasswörtern betrieben.
- Unsichere Default-Einstellungen der Endgeräte sind angepasst.
- Die lokale Konfiguration wird durch ein eigenes nicht triviales Passwort vor unbefugten Änderungen geschützt.
- IP-Telefone werden in einen Subnetz mit privaten IP-Adressen betrieben.
- Der Zugriff auf Remote-Schnittstellen des IP-Telefons ist, soweit die Konfiguration dies zulässt, auf ausgewählte Rechner eingeschränkt (siehe Prüfkriterium P 9).

- Eine standardkonforme Konfiguration der IP-Telefone wird in regelmäßigen Abständen überprüft.
- Die Integrität der Firmware wird durch Signaturen sichergestellt.
- Alle neuen Geräte werden vor dem Betrieb den Anforderungen entsprechend konfiguriert.

P 12 Einsatz von Profilen für Endgeräte

Das Kriterium ist erfüllt, wenn die Wahlmöglichkeiten und Leistungsmerkmale für Endgeräte über die Zuweisung von Profilen definiert werden können. Dabei sind die folgenden Szenarien zu berücksichtigen.

- Von einem öffentlich zugänglichen Telefon dürfen nur interne kostenfreie Nummern angerufen werden.
- Leistungsmerkmale die zusätzliche Kosten verursachen, werden individuell freigeschaltet.
- Endgeräte, die bezüglich ihrer Wahlmöglichkeiten und Leistungsmerkmale von den vorgesehenen abweichen, werden erkannt.

P 13 Patchmanagement

Das Kriterium ist erfüllt, wenn die folgenden Anforderungen beim Patchmanagement umgesetzt werden.

- Vor dem *Roll-Out* von Patches wird die Interoperabilität exemplarisch geprüft.
- Die Authentizität und Integrität der Patches ist sichergestellt.
- Veröffentlichte Sicherheitslücken werden zeitnah beseitigt oder Maßnahmen zur Absicherung getroffen.
- Die Vorgehensweise bei Patchvorgängen ist dokumentiert.
- Es muss beim *Roll-Out* berücksichtigt werden, dass gegebenenfalls die Änderungen rückgängig gemacht werden können.
- Eine Informationsbeschaffung über Sicherheitslücken für die betroffenen Systeme ist sichergestellt.

P 14 Authentifizierung der Endgeräte

Das Kriterium ist zum einen erfüllt, wenn eine Registrierung innerhalb der VoIP-Infrastruktur nur nach voriger Authentifizierung möglich ist. Zusätzlich muss ein dem Schutzbedarf angemessener Austausch der Authentifizierungsdaten erfolgen. Dabei sind die grundlegenden Dienste IP-Telefonie und *Mailbox* anhand der nachgenannten Kriterien zu überprüfen und für die Protokolle SIP, IAX und H.323 anhand der Tabelle 17 ein adäquates Verfahren zur sicheren Authentifizierung auszuwählen.

Protokoll	Schutzbedarf	
	normal	hoch
SIP	SIP-Digest	TLS
IAX	MD5	RSA
H.323	H.235.1	H.235.2/H.235.3

Tabelle 17: Verfahren zur sicheren Authentifizierung

- Der Abruf der Sprachnachrichten muss durch eine PIN geschützt sein.
- Das gewählte Passwort muss bezüglich der Komplexität hinreichend sicher gewählt werden[129].
- Um die Nicht-Abstreitbarkeit von Gesprächen sicherzustellen, müssen sich Nutzer durch eine PIN authentifizieren.
- Der Versuch eines nicht authentifizierten IP-Telefons ein Gespräch aufzubauen muss abgelehnt werden und bei den Protokollen SIP, IAX und H.323 mit einer der folgenden Nachrichten beantwortet werden.

Protokoll	Fehlermeldung
SIP	*401 Unauthorized* oder *Proxy Authentication Required*
IAX	*AUTHREQ*
H.323	*admissionReject (ARJ)*

Tabelle 18: Fehlermeldungen ohne vorherige Authentifizierung

[129] siehe Maßnahme M 2.11 „Regelung des Passwortgebrauchs“ [BSI05b, S. 845 ff, M 2.11]

P 15 Sichere Endgeräteauthentifizierung mittels IEEE 802.1X

Das Kriterium ist erfüllt, wenn die Authentifizierung der Endgeräte über IEEE 802.1X erfolgt und die folgenden Kriterien bei der Prüfung der Authentifizierung erfüllt werden.

- Der Zugang zum produktiven Netzwerk ist nur nach voriger Authentifizierung möglich.
- Werden Geräte nach fehlerhafter Authentifizierung in ein separates Netzsegment delegiert, dürfen keine Dienste der VoIP-Infrastruktur erreichbar sein.
- Fehlerhafte Login-Versuche werden protokolliert.
- Eine Multiportfunktion muss ebenfalls die portbasierte Authentifizierung nach IEEE 802.1X von den angeschlossenen Netzkomponenten fordern.
- Bei aktiviertem Multiport und umgesetzter Authentifizierung nach IEEE 802.1X können sich beide Endgeräte im Netzwerk authentifizieren.

P 16 Absicherung der Netzübergänge zu öffentlichen VoIP-Netzwerken

Das Kriterium ist erfüllt, wenn die Absicherung der Netzübergänge durch die im Folgenden genannten Kriterien erfolgreich überprüft wurde.

- Bei reiner IP-Telefonie müssen Gespräche in jedem Fall über die interne IP-Telefonanlage vermittelt werden.
- Bei hohem Schutzbedarf darf keine direkte Verbindung zu anderen VoIP-Netzwerken möglich sein, ferner muss diese durch einen SBC terminiert werden.
- Beim Einsatz eines IP-Gateways[130] müssen DoS-Angriffe durch eine Firewall oder SBC abgewehrt werden.
- Die für die Übertragung des RTP-Stroms notwendigen Ports müssen dynamisch durch ein ALG geöffnet werden.
- Die Funktionalität der Firewall und des NAT-Gateways muss auch unter bei erhöhter Netzlast sichergestellt sein.
- Die Firewall und der SBC müssen beim Einsatz von QoS-Protokollen[131], diese ebenfalls unterstützen.

P 17 Absichern der IP-Telefonanlage

Das Kriterium ist erfüllt, wenn die folgenden Kriterien zur „Härtung“ des Betriebssystems umgesetzt werden, bevor die IP-Telefonanlage in Betrieb genommen wird.

- Zur Funktion des Servers nicht benötigte Dienste sind zu deaktivieren und gegebenenfalls zu deinstallieren. Andernfalls ist der Zugriff durch eine Firewall einzuschränken (siehe Maßnahme M 16).
- Die Firewall-Einstellungen wurden bezüglich der ausgeführten Dienste angepasst.
- Es dürfen nur die zur Nutzung des Telefoniedienstes notwendigen Ports von anderen VoIP-Endgeräten erreichbar sein.
- Remote-Schnittstellen dürfen nur von ausgewählten Management-Stationen erreichbar sein (siehe Prüfkriterium P 9).
- Dienste der IP-PBX werden mit eingeschränkten Rechten ausgeführt, sofern darauf Einfluss genommen werden kann.
- Kritische Leistungsmerkmale wie eine externe Rufumleitung oder die Chefsekretärin-Funktion (Intercom-Funktion) sind standardmäßig deaktiviert und müssen individuell freigeschaltet werden.
- Nicht benötigter Benutzerkonten werden entfernt.
- Sensible TK-Daten werden verschlüsselt gespeichert.
- Ausführliches Logging ist aktiviert.
- Sichheitskritische Default-Einstellungen wurden überprüft und angepasst.
- HIDS läuft auf gehärteter IP-PBX, sofern dies die Konzeption der IP-PBX zulässt.

P 18 Absichern der Basis-Netzwerkdienste

Das Kriterium ist erfüllt, wenn Manipulationen von ARP- und DHCP-Nachrichten erkannt und für die VoIP-Infrastruktur dedizierte Basis-Netzwerkdienste betrieben werden.

[130] siehe Kapitel 3.2.3
[131] siehe Maßnahme M 5 „Bandbreitenmanagement“

P 19 USV für die Middleware

Das Kriterium ist erfüllt, wenn die unterbrechungsfreie Stromversorgung durch eine USV-Anlage für ausgewählte Komponenten sichergestellt ist.

- Die USV-Anlage ist den Anforderungen entsprechend dimensioniert und ermöglicht ein geregeltes Herunterfahren der Komponenten.
- Eine regelmäßige Wartung der USV-Anlage ist sichergestellt.
- Abhängig von den Anforderungen an die Verfügbarkeit müssen *Fail-Over-Mechanismen* den weiteren Betrieb der TK-Infrastruktur sicherstellen.

P 20 USV für IP-Telefone

Das Kriterium ist erfüllt, wenn das Telefonieren während eines Stromausfalls sichergestellt ist. Dazu müssen die folgenden Kriterien erfüllt werden.

- Die unterbrechungsfreie Stromversorgung der IP-Telefone wird durch PoE sichergestellt.
- Die unterbrechungsfreie Stromversorgung ist für weitere zur Aufrechterhaltung der Telefoniefunktion notwendige Komponenten sichergestellt.
- Beim Einsatz von PoE wird zusätzlich die Versorgung der PSE (Midspan) durch eine USV-Anlage sichergestellt.
- Die USV-Anlage ist für die zusätzliche Versorgung der IP-Telefone ausreichend dimensioniert.

P 21 Physische Zutrittskontrolle

Das Kriterium ist erfüllt, wenn der Zugang zu VoIP- und Netzwerkkomponenten wie IP-PBX, Switches und Router nur autorisiertem Personal möglich ist. Weiterhin muss die Zutrittskontrolle durch eine der folgenden Sicherheitsmechanismen sichergestellt werden. Für eine starke Zutrittskontrolle sind zwei der drei unten beschrieben Mechanismen anzuwenden[132].

- Zutrittskontrolle durch Besitz (Schlüssel und Schlüsselverwaltung oder Smartcards)
- Zutrittskontrolle durch Wissen (Passwort oder PIN)
- Zutrittskontrolle durch biometrische Merkmale (Fingerabdruck und Iris-Scan)

[132] siehe M 2.17 „Zutrittsregelung und -kontrolle“ [BSI05b, S. 852 ff.]

P 22 Sicherstellen der Notrufmöglichkeit

Das Kriterium ist erfüllt, wenn die Notrufmöglichkeit durch eine der folgenden Möglichkeiten sichergestellt ist.

- IP-Telefonie über PSTN-Gateway - Bei einem Stromausfall ist die Notrufmöglichkeit ebenfalls sicherzustellen.
- Telefon am Amtsanschluss
- Mobiltelefon

P 23 Einsatz von IDS

Das Kriterium ist erfüllt, wenn sowohl netzwerkbasierte als auch protokollspezifische Angriffe (siehe Kapitel A.3 Angriffsübersicht) auf die Module aus Kapitel 3.2 erkannt werden und eine Benachrichtigung des Administrators erfolgt. Die Angriffe lassen sich mit den in Kapitel A.1 beschriebenen *Audit-Tools* durchführen.

P 24 Maßnahmen gegen automatisierte unerwünschte Werbeanrufe

Das Kriterium ist erfüllt, wenn die folgenden Kriterien zum Schutz vor automatisierten Werbeanrufen umgesetzt wurden.

- Gespräche dürfen erst nach voriger Interaktion mit dem Sprachmenü durchgestellt werden.
- Das Sprachmenu muss sicherstellen, dass automatisierte Werbeanrufe den Gesprächspartner nicht erreichen und gebundene Ressourcen zeitnah wieder frei gegeben werden.

7 Schlussbetrachtungen

7.1 Zusammenfassung

Ziel dieser Arbeit war es, einen Maßnahmenkatalog mit zugehörigem Prüfschema auszuarbeiten, anhand dessen die Sicherheit in Voice over IP Installationen überprüft werden kann.

Dazu wird zu Beginn der Arbeit in die grundlegenden Eigenschaften der IP-Telefonie eingeführt und Unterschiede gegenüber der Festnetztelefonie und bestehenden Datennetzen aufgezeigt. Dies soll dem Leser einen ersten Einblick in die Thematik der IP-Telefonie geben und auf grundlegende Eigenschaften aufmerksam machen, die später in Gefährdungen und umzusetzenden Maßnahmen ein Rolle spielen. Dazu zählt von allen Dingen die Echtzeitcharakteristik von Sprache in Verbindung mit einer paketbasierten Übertragung. Diese Eigenschaft muss innerhalb der gemeinsamen Infrastruktur berücksichtigt werden, um den Anforderungen an Verfügbarkeit des Telefoniedienstes und der Qualität von Sprachübertragungen gerecht zu werden.

Im darauffolgenden Kapitel wird in die grundlegenden VoIP-Protokolle eingeführt. Dazu gehören zum einen Signalisierungsprotokolle (SIP, H.323, SCCP) und andererseits Protokolle zur Sprachübertragung (RTP). Zusätzlich existieren auch Protokolle wie IAX, welche die Übertragung der Signalisierung und der Sprache innerhalb einer Architektur ermöglichen. Grundsätzlich wird für die aktuell am Markt relevanten Protokolle eine Übersicht über deren Eigenschaften, Aufbau und Adressierungsmechanismen gegeben. Sofern die Offenlegung der Protokolle es ermöglicht hat, werden individuell die wesentlichen Kommunikationselemente und Nachrichtentypen der Protokolle anhand einer Beispielkommunikation erläutert.

Ferner wird auch in Protokolle zur verschlüsselten Übertragung der Signalisierung und der Sprachdaten sowie den für den Einsatz von SRTP notwendigen Schlüsselaustausch einführt. Diese Protokolle bilden bereits die wesentliche Grundlage für die sichere Übertragung der Sprache und werden im Maßnahmenkatalog neben weiteren Protokollen zur Verschlüsselung der Signalisierung für die Absicherung von Voice over IP Installationen eingesetzt. Durch die verschlüsselte Übertragung der Sprache können bereits zahlreiche Angriffe, wie die Manipulation und das Abhören von Kommunikationsverbindungen, unterbunden werden. Welche Protokolle eingesetzt werden können, hängt allerdings von der Unterstützung der Endgeräte ab. Folglich muss bereits bei der Auswahl der Komponenten auf eine Unterstützung von Sicherheitsmerkmalen geachtet werden.

Nach einer Einführung in die Grundlagen wird die für die Anwendung des Prüfschemas relevante Methodik vorgestellt. Dabei wird auf etablierte Verfahren der IT-Grundschutzvorgehensweise zurückgegriffen, die es ermöglichen, die anzuwen-

den Maßnahmen abhängig von der VoIP-Infrastruktur zu identifizieren (Modellierung) und die Sicherheitsdefizite zuverlässig zu bestimmen (Soll-Ist-Vergleich).

Um diese Methodik erfolgreich anwenden zu können, werden Module, ähnlich den Bausteinen der IT-Grundschutz-Kataloge, bereitgestellt. Diese umfassen Komponenten, die im allgemeinen in VoIP-Infrastrukturen eingesetzt werden. Für jedes Modul wird eine Gefährdungsübersicht gegeben und es werden die umzusetzenden Maßnahmen bestimmt.

Die Gefährdungen machen deutlich, dass VoIP nur erfolgreich sein kein, wenn neben der Verfügbarkeit und einer akzeptablen Sprachqualität auch die Sicherheit berücksichtigt wird. Ansonsten können Angriffe auf die VoIP-Infrastruktur zum Verlust der Verfügbarkeit führen und die Dienstgüte einschränken, so dass im Ergebnis kein Telefoniedienst zur Verfügung steht.

Bei den umzusetzenden Maßnahmen wird zwischen denen unterschieden, die bei einem normalen und hohen Schutzbedarf umzusetzen sind. Durch die Kategorisierung können abhängig vom individuellen Schutzbedarf der VoIP-Infrastruktur spezifische Maßnahmen als Referenz bereitgestellt werden. Die Maßnahmen sind Bestandteil des entwickelten Maßnahmenkataloges, der herstellerunabhängig *Best-Practice-Verfahren* zur Verfügung stellt, die zum einen Gefährdungen bei der Übertragung über IP-basierte Netze und Gefährdungen der Festnetztelefonie beseitigen. Zusätzlich werden Maßnahmen zur Absicherung von VoIP-spezifischen Gefährdungen bereitgestellt. Gleichzeitig wird durch die in den Maßnahmen beschriebenen Anforderungen festgelegt, welche Ansätze zur Umsetzung der Maßnahme gewählt werden können und welche Kriterien erfüllt werden müssen.

Durch die in dieser Arbeit für jede Maßnahme entwickelten Prüfkriterien wird sichergestellt, dass eine umfassende Ermittlung der Sicherheitsdefizite in einem Soll-Ist-Vergleich erfolgen kann. Die Sicherheitsdefizite bilden die Grundlage für die Umsetzung der defizitären Maßnahmen.

Die Arbeit leistet somit einen wesentlichen Beitrag zur Bewertung der Sicherheit in VoIP-Infrastrukturen. Dabei bildet der entwickelte Maßnahmenkatalog eine allgemeingültige Referenz für die Bewertung und Absicherung von VoIP-Infrastrukturen.

7.2 Ausblick

Bereits zum jetzigen Zeitpunkt hängt die Sicherheit der VoIP-Infrastruktur wesentlich von der des Datennetzes ab. In Zukunft wird es aufgrund der Konvergenz der Anwendungen immer schwieriger werden, Sprach- und Datennetz zu trennen. Somit müssen Sicherheitskonzepte zunehmend die Gefährdungen der ganzen Infrastruktur berücksichtigen und Maßnahmen zur Absicherung für das gemeinsame IP-Netzwerk bereitstellen.

Bei der Unterstützung von VoIP-Protokollen zeichnet sich zunehmend ab, dass SIP herstellerübergreifend in Form sogenannter *dual-mode* IP-Telefone neben proprietären Protokollen genutzt wird. Die Hersteller werden aktuell zunehmend den Anforderungen an Protokolle zur Verschlüsselung der Daten gerecht. Diese umfassen im Umfeld von SIP den Einsatz von TLS und SRTP zur Verschlüsselung. Sie erfüllen in den zur Zeit vorwiegend betriebenen Insellösungen die Anforderung an eine Verschlüsselung des gesamten Datenstroms, da nur die Verbindung zur IP-Telefonanlage abgesichert werden muss.

Wenn zunehmend die Übertragung der Daten Ende-zu-Ende über das Internetprotokoll erfolgt, müssen weitere Mechanismen in den Endgeräten integriert werden, die eine Ende-zu-Ende-Verschlüsselung der Signalisierung ermöglichen. Diese Verfahren werden notwendig, da auch VoIP-Betreiber Mechanismen zur Vorratsdatenspeicherung bereitstellen müssen [Kre06]. Die Grundannahme, dass beim Einsatz einer *Hop-by-Hop-Verschlüsselung* der nächste Hop vertrauenswürdig sein muss, ist somit nicht sichergestellt.

Neben den Anforderungen an Sicherheitsmechnismen wird es, je mehr Endgeräte existieren und je verteilter diese zum Einsatz kommen, immer schwieriger werden, eine Vertrauensbeziehung untereinander aufzubauen und zu verwalten. Die Einrichtung einer zentralen PKI, die eine Vertrauensbeziehung zwischen den Nutzern herstellt, hat sich im Bereich der E-Mail-Kommunikation bisher nur in firmeninternen Lösungen durchgesetzt. Um eine sichere Ende-zu-Ende-Kommunikation über das Internetprotokoll zu ermöglichen, müssen daher Lösungen angeboten werden, die eine Vertrauensbeziehung durch den Schlüsselaustausch zwischen den Nutzern herstellen, ähnlich dem Ansatz von ZRTP. Durch die Vielzahl der Protokolle müssen diese Lösungen hersteller- und protokollunabhängig den Einsatz von Sicherheitsmechanismen erlauben.

Zusätzlich zu der in dieser Arbeit vorwiegend berücksichtigten technischen und organisatorischen Sicherheit von VoIP müssen die Nutzer zusätzlich, ähnlich wie bei der Nutzung von E-Mail, für die Gefährdungen sensibilisiert werden. Wenn dies erfolgt, können sie zusätzlich zur Sicherheit der VoIP-Infrastruktur beitragen.

Abkürzungsverzeichnis

ACF	Admission Confirmation
AES	Advanced Encryption Standard
ALG	Application Layer Gateway
ARJ	Admission Reject
ARP	Address Resolution Protocol
ARQ	Admission Request
ATM	Asynchronous Transfer Mode
BRQ	Bandwidth Change Request
BSI	Bundesamt für Sicherheit in der Informationstechnik
CoS	Class of Service
CSRC	Contributing Source
CTI	Computer Telephony Integration
CU	Currently Unused
DAI	Dynamic ARP Inspection
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DMZ	Demilitarisierte Zone
DoS	Denial of Service
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DTMF	dual tone multi-frequency
EAP	Extensible Authentication Protocol
EOFB	Enhanced Output Feedback Mode
ESP	Encapsulated Security Payload
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IAX	Inter-Asterisk eXchange
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange

IntServ Integrated Services
IPSec Internet Protocol Security
ISP Internet-Service-Provider
ITU International Telecommunication Union

LAN Local Area Network

MCU Multipoint Control Unit
MIKEY Multimedia Internet KEYing
MitM Man-in-the-Middle
MKI Master Key Identifier
MPLS Multiprotocol Label Switching

NAT Network Address Translation
NIDS Network Intrusion Detection System
NIST National Institute of Standards and Technology

OUSPG Oulu University Secure Programming Group

PD Power Device
PHB Per-Hop-Behavior
PKI Public Key Infrastruktur
PoE Power over Ethernet
PSE Power Source Equipment
PSTN Public Switched Telefon Network

QoS Quality of Service

RADIUS Remote Authentication Dial In User Service
RAS Registration Admission and Status
RSVP Resource Reservation Protocol
RTCP Real Time Control Protocol
RTP Real-Time Transport Protocol

SAS Short Authentication String
SBC Session Border Controller
SCCP Skinny Client Control Protocol
SDES Security Descriptions
SDP Session Description Protocol
SIP Session Initiation Protocol
SIPS SIP Secure
SNMP Simple Network Management Protocol

SPIT Spam over Internet Telephony
SRTP Secure Real-time Transport Protocol
SSH Secure Shell
SSRC Synchronisation Source

TCI Tag Control Information
TCP Transmission Control Protocol
TEK Traffic-encrypting Key
TFTP Trivial File Transfer Protocol
TGK TEK Generation Key
TLS Transport Layer Security
TOS Type of Service

UA User Agent
UAC User Agent Client
UAS User Agent Server
UDP User Datagram Protocol
URI Uniform Resource Identifier
USV Unterbrechungsfreie Stromversorgung

VID VLAN-ID
VLAN Virtual Local Area Network
VoIP Voice over IP
VOIPSA Voice over IP Security Alliance
VRRP Virtual Router Redundancy Protocol

WLAN Wireless LAN
WPA Wi-Fi Protected Access

Literatur

[AAG+05] Adelsbach, André ; Alkassar, Ammar ; Garbe, Karl-Heinz ; Luzaic, Mirko ; Manulis, Mark ; Scherer, Edgar ; Schwenk, Jörg ; Siemens, Eduard: *VoIPSEC : Studie zur Sicherheit von Voice over Internet Protocol*. Köln : Bundesanzeiger Verlag, 2005 (Voice over IP : sichere Umstellung der Sprachkommunikation auf IP-Technologie). – 173 S. http://www.bsi.de/literat/studien/VoIP/index.htm. – ISBN 3–89817–539–1

[ABW06] Andreasen, F. ; Baugher, M. ; Wing, D.: RFC 4568 - Session Description Protocol (SDP) Security Descriptions for Media Streams / The Internet Society. Version: Juli 2006. http://www.ietf.org/rfc/rfc4568.txt

[AC03] Aboba, B. ; Calhoun, P.: RFC 3579 - RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP) / The Internet Society. Version: September 2003. http://www.ietf.org/rfc/rfc3579.txt

[ACL+04] Arkko, J. ; Carrara, E. ; Lindholm, F. ; Naslund, M. ; Norrman, K.: RFC 3830 - MIKEY: Multimedia Internet KEYing / The Internet Society. Version: August 2004. http://www.ietf.org/rfc/rfc3830.txt

[Bac06] Bacso, Nikolett: *Secure Computing Warns of New VoIP Based Phishing Scam*. Version: Juli 2006. http://www.securecomputing.com/press_releases.cfm?p=irol-newsArticle&ID=879984. – Secure Computing Corporation

[BBC+98] Blake, S. ; Black, D. ; Carlson, M. ; Davies, E. ; Wang, Z. ; Weiss, W.: RFC 2475 - An Architecture for Differentiated Services / The Internet Society. Version: Dezember 1998. http://www.ietf.org/rfc/rfc2475.txt

[BI04] BGBl I 2004, 1190: *Telekommunikationsgesetz*. Version: 2004. http://www.gesetze-im-internet.de/tkg_2004. – zuletzt geändert am 7.7.2005

[BIT06] BITKOM: *Internet-Telefonie: Privatnutzer haben die Nase vorn*. Version: Oktober 2006. http://www.bitkom.de/de/presse/30739_42026.aspx

[BMN+04] Baugher, M. ; McGrew, D. ; Naslund, M. ; Carrara, E. ; Norrman, K.: RFC 3711 - The Secure Real-time Transport Protocol (SRTP) / The Internet Society. Version: März 2004. http://www.ietf.org/rfc/rfc3711.txt

[BR06] Benz, Benjamin ; Reimann, Lars: *Fiktive Netzwerke : Netze schützen mit VLANs*. Version: September 2006. http://www.heise.de/netze/artikel/print/77832. Heise Zeitschriften Verlag

[BSI98] BSI: *Sicherer Einsatz von digitalen Telekommunikationsanlagen : Version 2*. Köln : Bundesanzeiger Verlag, 1998 (Schriftenreihe zur IT-Sicherheit - Band 1 - BSI 6001). – 79 S. http://www.bsi.de/literat/tkanlage/6001.pdf. ISSN 0947–093X

[BSI05a] BSI: *BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise*. Köln : Bundesanzeiger Verlag, 2005 (IT-Sicherheitsmanagement und IT-Grundschutz : BSI-Standards zur IT-Sicherheit 1.0). http://www.bsi.de/literat/bsi_standard/standard_1002.pdf. – ISBN 3–89817–547–2

[BSI05b] BSI: *IT-Grundschutz-Kataloge*. Köln : Bundesanzeiger Verlag, 2005 (IT-Grundschutzkataloge : Standardwerk zur IT-Sicherheit). http://www.bsi.de/gshb/deutsch/download/itgshb_2005.pdf

[BW02] Blumenthal, U. ; Wijnen, B.: RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) / The Internet Society. Version: Dezember 2002. http://www.ietf.org/rfc/rfc3414.txt

[CE06] Collier, Mark ; Endler, David: *Hacking Exposed VoIP*. Version: 2006. http://www.hackingvoip.com/sec_tools.html

[Cis] Cisco Systems Inc. (Hrsg.): *Catalyst 6500 Series - Switch Cisco IOS Software Configuration Guide*. Release 12.2SX. San Jose: Cisco Systems Inc., http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a00801609ea.html. – Chapter 38/39 - Configuring DHCP Snooping und Configuring Dynamic ARP Inspection (DAI)

[CP000] *Internetworking Technology Handbook*. Bd. 3. Indianapolis : Cisco Press, 2000. – 1077 S. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.pdf. – ISBN 1–58705–001–3. – Chapter 56 - Simple Network Management Protocol

[DA01] Droms, R. ; Arbaugh, W.: RFC 3118 - Authentication for DHCP Messages / The Internet Society. Version: Juni 2001. http://www.ietf.org/rfc/rfc3118.txt

[Dav06] Davies, Martyn: *Not Just SPIT but SPOG and SPOM*. http://voipsa.org/blog/2006/06/15/not-just-spit-but-spog-and-spom. Version: 2006

[DIS06] DISA: INTERNET PROTOCOL TELEPHONY & VOICE OVER INTERNET PROTOCOL - SECURITY TECHNICAL IMPLEMENTATION GUIDE / Department of Defense. Version: April 2006. http://iase.disa.mil/stigs/stig/VoIP-STIG-V2R2.pdf (Version 2, Release 2)

[EGJ+05] Endler, David ; Ghosal, Dipak ; Jafari, Reza ; Karlcut, Akbal ; Kolenko, Marc ; Nguyen, Nhut ; Walkoe, Wil ; Zar, Jonathan: VoIP Security and Privacy Threat Taxonomy / Voice over IP Security Alliance (VOIPSA). Version: Oktober 2005. http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

[Euc06] Euchner, M.: RFC 4650 - HMAC-Authenticated Diffie-Hellman for Multimedia Internet KEYing (MIKEY) / The Internet Society. Version: September 2006. http://www.ietf.org/rfc/rfc4650.txt

[FHBH+99] Franks, J. ; Hallam-Baker, P. ; Hostetler, J. ; Lawrence, S. ; Leach, P. ; Luotonen, A. ; Stewart, L.: RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication / The Internet Society. Version: Juni 1999. http://www.ietf.org/rfc/rfc2617.txt

[FI06] Fries, S. ; Ignjatic, D.: On the applicability of various MIKEY modes and extensions / The Internet Society. Version: August 2006. http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-applicability-02.txt. – draft-ietf-msec-mikey-applicability-02

[FS99] Follows, Jonathan ; Straeten, Detlef: *Application-Driven Networking: Class of Service in IP, Ethernet, and ATM Networks*. IBM Redbooks, 1999. – 162 S. http://www.redbooks.ibm.com/redbooks/pdfs/sg245384.pdf. – ISBN 0738414522

[GL06] Glemser, Tobias ; Lorenz, Reto: *Weakness in implemenation of proccessing SIP-Notify-Messages in VoIP-Phones*. Version: Juli

2006. http://pentest.tele-consulting.com/advisories/05_07_06_voip-phones.txt. Tele-Consulting GmbH Advisory

[GLW+05] Grow, Robert M. ; Law, David J. ; William, Wael ; Steven, Diab ; Carlson, B. ; Dawe, Piers: 802.3af - IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - SECTION TWO - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications / IEEE Computer Society. Version: Dezember 2005. http://standards.ieee.org/getieee802/download/802.3-2005_section2.pdf

[Gra01] Granger, Sarah: Social Engineering Fundamentals, Part I: Hacker Tactics. (2001), Dezember. http://www.securityfocus.com/infocus/1527

[Hal03] Halpern, Jason: *IP Telephony Security in Depth*. Version: 2003. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.pdf. SAFE Blueprint. – 61 S. – Cisco Systems

[HC98] Harkins, D. ; Carrel, D.: RFC 2409 - The Internet Key Exchange (IKE) / The Internet Society. Version: November 1998. http://www.ietf.org/rfc/rfc2409.txt

[Hin04] Hinden, R.: RFC 3768 - Virtual Router Redundancy Protocol (VRRP) / The Internet Society. Version: April 2004. http://www.ietf.org/rfc/rfc3768.txt

[HSSR99] Handley, M. ; Schulzrinne, H. ; Schooler, E. ; Rosenberg, J.: RFC 2543 - SIP: Session Initiation Protocol / The Internet Society. Version: März 1999. http://www.ietf.org/rfc/rfc2543.txt

[HWPT05] Hoff, Simon ; Wetzlar, Joachim ; Pütz, Wilhelm ; Ternes, Berthold ; BSI (Hrsg.): *Technische Richtlinie Sicheres WLAN : (TR-S-WLAN)*. SecuMedia, 2005. – 416 S. – ISBN 3–922746–70–5

[IT00] ITU-T: ITU-T Recommendation H.235 - Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals / ITU-T

[IT05a] ITU-T: ITU-T Recommendation H.235.0 - H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems / ITU-T

[IT05b] ITU-T: ITU-T Recommendation H.235.1 - H.323 security: Baseline security profile / ITU-T

[IT05c] ITU-T: ITU-T Recommendation H.235.2 - H.323 security: Signature security profile / ITU-T

[IT05d] ITU-T: ITU-T Recommendation H.235.3 - H.323 security: Hybrid security profile / ITU-T

[IT05e] ITU-T: ITU-T Recommendation H.235.4 - H.323 security: Direct and selective routed call security / ITU-T

[IT05f] ITU-T: ITU-T Recommendation H.235.5 - H.323 security: Framework for secure authentication in RAS using weak shared secrets / ITU-T

[IT05g] ITU-T: ITU-T Recommendation H.235.6 - H.323 security: Voice encryption profile with native H.235/H.245 key management / ITU-T

[IT05h] ITU-T: ITU-T Recommendation H.235.7 - Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235 / ITU-T

[IT05i] ITU-T: ITU-T Recommendation H.235.8 - Key exchange for SRTP using secure signalling channels / ITU-T

[IT05j] ITU-T: ITU-T Recommendation H.235.9 - Security gateway support for H.323 / ITU-T

[IT06a] ITU-T: ITU-T Recommendation H.225.0 - Control protocol for multimedia communication / ITU-T

[IT06b] ITU-T: ITU-T Recommendation H.245 - Call signalling protocols and media stream packetization for packet-based multimedia communication systems / ITU-T

[IT06c] ITU-T: ITU-T Recommendation H.323 (Version 6) Prepublished version - Packet-based multimedia communications systems / ITU-T

[Jam02] James, Anthon: Using IEEE 802.1x to Enhance Network Security. (2002). http://www.foundrynet.com/pdf/wp-ieee-802.1x-enhance-network.pdf

[JCS04a] Jeffree, Tony ; Congdon, Paul ; Sala, Dolors: 802.1X - IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control / IEEE Computer Society. Version: November 2004. http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

[JCS04b] Jeffree, Tony ; Congdon, Paul ; Seaman, Mick: 802.1D - IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges / IEEE Computer Society. Version: Februar 2004. http://standards.ieee.org/getieee802/download/802.1D-2004.pdf

[JP06] Johnston, Alan B. ; Piscitello, David M.: *Understanding Voice Over IP Security*. Boston : Artech House Telecommunications Library, 2006. – 261 S. – ISBN 1–596–93050–0

[KA98a] Kent, S. ; Atkinson, R.: RFC 2401 - Security Architecture for the Internet Protocol / The Internet Society. Version: November 1998. http://www.ietf.org/rfc/rfc2401.txt

[KA98b] Kent, S. ; Atkinson, R.: RFC 2406 - IP Encapsulating Security Payload (ESP) / The Internet Society. Version: November 1998. http://www.ietf.org/rfc/rfc2406.txt

[Kre06] Krempl, Stefan: *EU-Richtlinie zur Vorratsspeicherung tritt in Kraft*. Version: April 2006. http://www.heise.de/newsticker/meldung/print/72031. Heise Zeitschriften Verlag

[KWF05] Kuhn, D. R. ; Walsh, Thomas J. ; Fries, Steffen: *Security Considerations for Voice Over IP Systems*. Version: Januar 2005. http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf. National Institute of Standards and Technology (NIST)

[Lon01] Lonvick, C.: RFC 3164 - The BSD syslog Protocol / The Internet Society. Version: August 2001. http://www.ietf.org/rfc/rfc3164.txt

[LS03] Lidinsky, William P. ; Seaman, Mick: 802.1Q - IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks / IEEE Computer Society. Version: Mai 2003. http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf

[Mat06] Materna, Bogdan: *A Proactive Approach to VoIP Security*. Version: März 2006. http://www.voipshield.com/images/

PDFs/a%20proactive%20approach%20to%20voip%20security_whitepaper.pdf. VoIPshield Systems

[Mih05] Mihai, Amarandei-Stavila: Voice over IP Security - A layered approach / Xmco Partners. Version: Juli 2005. http://www.xmcopartners.com/whitepapers/voip-security-layered-approach.pdf

[NBBB98] Nichol, K. ; Blake, S. ; Baker, F. ; Black, D.: RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers / The Internet Society. Version: Dezember 1998. http://www.ietf.org/rfc/rfc2474.txt

[NR01] New, D. ; Rose, M.: RFC 3195 - Reliable Delivery for syslog / The Internet Society. Version: November 2001. http://www.ietf.org/rfc/rfc3195.txt

[Pet04] Peterson, J.: RFC 3853 - S/MIME Advanced Encryption Standard (AES) - Requirement for the Session Initiation Protocol (SIP) / The Internet Society. Version: Juli 2004. http://www.ietf.org/rfc/rfc3853.txt

[Poi05] Pointon, Adam: *Asterisk Voicemail Unauthorized Access Vulnerability*. Version: November 2005. http://www.securityfocus.com/bid/15336/info. www.securityfocus.com

[Por06] Porter, Thomas: *Practical VoIP Security*. Rockland : Syngress Publishing, 2006. – 500 S. – ISBN 1–597–49060–1

[RF03] Rafail, Jason A. ; Finlay, Ian A.: *Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP)*. Version: Februar 2003. http://www.cert.org/advisories/CA-2003-06.html. CERT® Advisory

[RJP06] Rosenberg, J. ; Jennings, C. ; Peterson, J.: The Session Initiation Protocol (SIP) and Spam / The Internet Society. Version: März 2006. http://tools.ietf.org/wg/sipping/draft-ietf-sipping-spam/draft-ietf-sipping-spam-02.txt. – draft-ietf-sipping-spam-02

[RMKGEL96] Rekhter, Y. ; Moskowitz, B. ; Karrenberg, D. ; Groot E. Lear, G. J.: RFC 1918 - Address Allocation for Private Internets / The Internet Society. Version: Februar 1996. http://www.ietf.org/rfc/rfc1918.txt

[RS02a] Rosenberg, J. ; Schulzrinne, H.: RFC 3263 - Session Initiation Protocol (SIP): Locating SIP Servers / The Internet Society. Version: Juni 2002. http://www.ietf.org/rfc/rfc3263.txt

[RS02b] Rosenberg, J. ; Schulzrinne, H.: RFC 3264 - An Offer/Answer Model with the Session Description Protocol (SDP) / The Internet Society. Version: Juni 2002. http://www.ietf.org/rfc/rfc3264.txt

[RSC+02] Rosenberg, J. ; Schulzrinne, H. ; Camarillo, G. ; Johnston, A. ; Peterson, J. ; Sparks, R. ; Handley, M. ; Schooler, E.: RFC 3261 - SIP: Session Initiation Protocol / The Internet Society. Version: Juni 2002. http://www.ietf.org/rfc/rfc3261.txt

[RTH+06] Rohwer, Thomas ; Tolkmit, Carsten ; Hansen, Marit ; Hansen, Markus ; Möller, Jan ; Waack, Henning: *Abwehr von „Spam over Internet Telephony"(SPIT-AL).* Version: Januar 2006. http://www.spit-abwehr.de/Whitepaper_SPITAL_20060310.pdf. TNG – THE NET GENERATION AG

[SCFJ03] Schulzrinne, H. ; Casner, S. ; Frederick, R. ; Jacobson, V.: RFC 3550 - RTP: A Transport Protocol for Real-Time Applications / The Internet Society. Version: Juli 2003. http://www.ietf.org/rfc/rfc3550.txt

[SCG+06] Spencer, M. ; Capouch, B. ; Guy, E. ; Miller, F. ; Shumard, K.: IAX: Inter-Asterisk eXchange Version 2 / The Internet Society. – draft-guy-iax-01

[SIP05] *Sipgate startet bundesweiten VoIP-Notruf.* Version: Juli 2005. http://www.heise.de/newsticker/meldung/print/61567. Heise Zeitschriften Verlag

[TAO06a] Trick, Ulrich ; Akkaya Özgür ; Oehler, Steffen: Notruf bei VoIP - heutige Situation und Problemstellung. In: *ntz* 2 (2006), S. 36–39

[TAO06b] Trick, Ulrich ; Akkaya Özgür ; Oehler, Steffen: Notruf bei VoIP - Lösungsmöglichkeiten. In: *ntz* 3-4 (2006), S. 24–27

[TW05] Trick, U. ; Weber, F.: *SIP, TCP/IP und Telekommunikationsnetze : Next Generation Networks und VoIP - konkret.* 2. Oldenbourg Verlag München Wien, 2005. – 499 S. – ISBN 3–486–57796–4

[Wal05] Wallingford, Theodore ; Loukides, Michael K. (Hrsg.): *Switching to VoIP : A Solutions Manual for Network Professionals*. Bd. 1. Beijing : O'Reilly, 2005. – 477 S. – ISBN 0–596–00868–6

[Win06] Wing, Dan: *Overview of SIP Media Security Options*. Version: März 2006. http://www3.ietf.org/proceedings/06mar/slides/raiarea-1/raiarea-1.ppt. 65 IETF meeting

[ZJC06] Zimmermann, P. ; Johnston, A. ; Callas, J.: ZRTP: Extensions to RTP for Diffie-Hellman Key Agreement for SRTP / The Internet Society. Version: März 2006. http://www.philzimmermann.com/docs/draft-zimmermann-avt-zrtp-01.html. – draft-zimmermann-avt-zrtp-01

Abbildungsverzeichnis

Tabellenverzeichnis

A Anhang

A.1 Audit-Tools zur Schwachstellenanalyse

Im Rahmen dieses Kapitels sollen Tools vorgestellt werden, mit dessen Hilfe es möglich ist, Prüfkriterien und damit gezielt die Umsetzung bestimmter Maßnahmen zu überprüfen.

A.1.1 allgemeine Tools

- Whireshark (Protokoll- und Netzwerkanalyse)[133]
- Nmap (Portscanner)[134]
- Dsniff (MitM-Angriff)[135]

A.1.2 VoIP-spezifische Tools

- SipSak[136]
- SivuS[137]
- Smap[138]
- VOMIT[139]
- SIPcrack[140]
- Voipong[141]
- VoIP Security Tools[142]

[133] www.wireshark.org
[134] www.insecure.org/nmap
[135] www.monkey.org/ dugsong/dsniff
[136] www.sipsak.org
[137] www.vopsecurity.org
[138] www.wormulon.net/files/pub/smap-0.4.1.tar.gz
[139] http://vomit.xtdnet.nl
[140] www.remote-exploit.org/index.php/Sipcrack
[141] www.enderunix.org/voipong
[142] www.hackingvoip.com/tools.html

A.2 Hersteller von VoIP-Endgeräten

Hersteller	URL	unterstützte VoIP-Protokolle
Cisco	www.cisco.de	SCCP und SIP
Snom	www.snom.de	SIP
Mitel	www.mitel.com	MiNET und SIP
3Com	www.3com.com/voip	NBX und SIP
Grandstream	www.grandstream.com	SIP
Shoretel	www.shoretel.com	MGCP
Avaya	www.avaya.de	SIP
Siemens	www.siemens.de/hipath	CorNet-IP/H.323 und SIP
Nortel	www.nortel.com	UNIStim
NEC Infrontia	www.nec-i.de	H.323
Atcom	www.atcom.cn	MGCP, H.323, IAX2 und SIP

Tabelle 19: Hersteller von VoIP-Endgeräten

A.3 Angriffsübersicht

A.3.1 Netzwerkbasierte Angriffe

Angriff	Kategorie	Angriffsschicht	Verweis GSHB
ARP-Spoofing	Abhören (MitM)	Layer 2	G 5.112
MAC-Flooding	Abhören (MitM)	Layer 2	G 5.112
Route Injection	Abhören (MitM)	Layer 3	G 5.51
DNS-Spoofing	Abhören (MitM)	Layer 4	G 5.78
VLAN-Angriff	Verfügbarkeit (Dos)	Layer 2	G 5.115
MAC-Spoofing	Verfügbarkeit (Dos)	Layer 2	G 5.113
DHCP-Starvation	Verfügbarkeit (Dos)	Layer 3	
Ping Flooding	Verfügbarkeit (Dos)	Layer 3	
SYN-Flooding	Verfügbarkeit (Dos)	Layer 4	
LAND-Flooding	Verfügbarkeit (Dos)	Layer 4	
STP-Angriff	MitM & DoS	Layer 2	G 5.114
DHCP Rogue Server	MitM & DoS	Layer 3	
ICMP-Redirect	MitM & DoS	Layer 3	G 5.50
IP-Spoofing	Verfügbarkeit (Dos) & Identitätsfälschung	Layer 3	G 5.48

Tabelle 20: Netzwerkbasierte Angriffe [AAG+05; BSI05b]

A.3.2 Protokollspezifische Angriffe

Angriff	Protokoll	Verweis Threat Taxonomy
Spoofing	SIP	[EGJ+05, Kap. 6.7]
Request Flooding	SIP[a],IAX	[EGJ+05, Kap. 8.1.1.1.3]
Call Termination	SIP[b]	[EGJ+05, Kap. 8.1.1.4.1]
Call Hijacking	SIP[c]	[EGJ+05, Kap. 8.1.1.5.2]
Registration Hijacking	SIP	[EGJ+05, Kap. 8.1.1.5.1]
Rogue Server	alle	[EGJ+05, Kap. 8.1.1.5.3]
Digest-Cracking	SIP	
Fuzzing	H.323 & SIP	[EGJ+05, Kap. 8.1.2.2.3]
Call Flooding	RTP	[EGJ+05, Kap. 8.1.1.1.1]
Insertion Attack	RTP & RTCP	[EGJ+05, Kap. 6.4]
Bid-Down Attack	SRTP	

Tabelle 21: Protokollspezifische Angriffe [GL06; Mih05; CE06]

[a] Invite, Register
[b] SIP-CANCEL & -BYE
[c] 301 Moved Permanently & 302 Moved Temporarily

Eidesstattliche Erklärung

Ich versichere, dass ich diese Diplomarbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Brandenburg, 4. Dezember 2006

Paul Lange