

Universität
Rostock



Traditio et Innovatio

Universität Rostock

Fakultät für Informatik und Elektrotechnik

Institut für Informatik

Lehrstuhl für Informations- und Kommunikationsdienste

Bachelorarbeit

Sichere Installation von VoIP-Telefonanlagen

eingereicht am

01. April 2011

von

Georg Limbach

Matrikel-Nr. 7201071

Betreuer:

Dr.-Ing. Thomas Mundt (Institut für Informatik, Universität Rostock)

Inhaltsverzeichnis

1. Einführung	1
1.1. Probleme der VoIP-Sicherheit	1
1.2. Schwächen im System finden und korrigieren	2
1.3. Beispiel eines Ablaufs mit Hinweisen zur Arbeit	2
2. Bedrohungsanalyse	4
2.1. Übersicht über Bedrohungen einer VoIP-PBX	4
2.2. Bedrohung auf Ebene des Netzwerks	5
2.3. Bedrohungen durch Gateways und Protokolle	15
2.4. Risiken durch Betriebssystem	16
2.5. Risiken im Bezug auf Hardware	17
2.6. Bedrohungen auf Anwendungsebene	18
2.6.1. Programme mit Schadensfunktion	18
2.6.2. VoIP-Endgeräte	19
2.6.3. VoIP-Middleware	20
2.6.4. WLAN	22
3. Sicherheitsmaßnahmen	24
3.1. Sicherheit der Netzstruktur und ihre Komponenten	25
3.2. Dienstgüte und Netzmanagement	29
3.3. Besondere Maßnahmen für Notrufe	30
3.4. Aspekte im Zusammenhang mit Protokollen	32
3.5. Firewalls und NIDS zur Sicherung des Netzwerkes nach außen	34
3.6. Maßnahmen für VoIP-Komponenten im Netzwerk	35
3.7. Protokolle	35
4. Expertensystem	38
4.1. Allgemeiner Ablauf des Programms	38
4.2. Hinweise zur Leistungsfähigkeit der Software	39
4.3. Ansätze für Datenerhebung	40
4.4. Interaktion des Benutzers mit der Software	43

Inhaltsverzeichnis

5. Zusammenfassung	48
5.1. Ausblick	48
5.2. Fazit	48
A. Quellcode	50
Abbildungsverzeichnis	55
Tabellenverzeichnis	56
Literaturverzeichnis	57

1. Einführung

1.1. Probleme der VoIP-Sicherheit

Netzwerke und Rechnersysteme werden zunehmend Ziel von bösartigen Angriffen. Die sorgfältige Planung und Überwachung von VoIP¹-Installationen wird dadurch immer bedeutender. Wie bei jedem Computersystem ist auf die Informationssicherheit zu achten.

Jeder Administrator sollte um die Anfälligkeit seines VoIP-Systems besorgt sein. Im Folgenden werden die wichtigsten Merkmale aufgelistet, die bei jeder Konfiguration sicher gestellt werden müssen.

Vertraulichkeit

Unter Vertraulichkeit versteht man den Schutz der Informationen vor unbefugtem Zugriff. Im Bereich der Telekommunikation über IP-Netze kann an verschiedenen Stellen die Vertraulichkeit verletzt werden. Somit könnten Telefonate abgehört oder mitgeschnitten werden. Außerdem würde auch eine Herausgabe von Voicemails an falsche Personen zu einem Vertraulichkeitsverlust führen.

Integrität

Die Integrität bezeichnet den Schutz der Information vor unbefugter Veränderung. Gebührenbetrug und Vertraulichkeitsverlust können eintreten, wenn die Unversehrtheit der Verbindung gestört wird.

¹Voice-over-IP

1. Einführung

Authentizität

Die Authentizität von Daten beweist deren Echtheit im Bezug auf den Absender. Es sollte immer sichergestellt werden, dass Information wirklich von dem angegebenen Absender stammen. Gelingt eine Täuschung, sind falsche Steuerinformationen oder ein Gebührenbetrug mögliche Folgen.

Verfügbarkeit

Die Verfügbarkeit bezeichnet den Umstand das ein System zur Verfügung steht und nicht dauerhaft beeinträchtigt ist. Ein DoS-Angriff² oder eine Überlastung des Systems könnte eine Einschränkung der Verfügbarkeit auslösen.

1.2. Schwächen im System finden und korrigieren

Die Schwierigkeit für einen Administrator eines VoIP-Systems besteht in dem Finden von Unzulänglichkeiten der Sicherheit. Eine Checkliste mit Bedrohungen und Lösungsvorschlägen sollte in jeder VoIP-Umgebung bereitgehalten werden. Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) stellt den IT-Grundschutzkatalog [BSI09] bereit. Einige Prüffragen und Kontrollen sind dort für VoIP enthalten.

Jeder Wissensbegierige muss sich zuerst in den Katalog einlesen und die für ihn wichtigen Passagen finden. Nicht jeder Manager eines Systems hat dafür Zeit. Deshalb stellt sich die Frage, ob es ein Programm geben kann, dass diese Arbeit vereinfacht. Mit dieser Frage befasst sich diese Arbeit.

1.3. Beispiel eines Ablaufs mit Hinweisen zur Arbeit

Für ein Programm, welches Maßnahmen selbstständig vorschlagen soll, sind besonders die Eingaben wichtig. Der Benutzer muss sehr genaue und dem System verständliche Angaben bereitstellen.

In Abbildung 1.1 wird ein grobes Schema der Ein- und Ausgaben des Systems gezeigt. Die Angaben von Systembeschreibung (1) und Anforderungen (2) sind durch die Vielzahl der zur Verfügung stehenden Konfigurationen sehr komplex. In Kapitel 2 werden Gefahren (3) aufgezählt, die für Datensicherheit relevant sind. Durch diese

²Denial of Service, zu Deutsch: Dienstblockade

1. Einführung

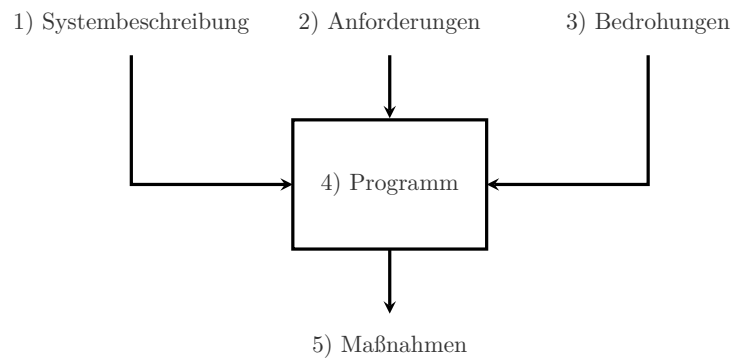


Abbildung 1.1.: Ein- und Ausgaben des Systems

Daten können die Angaben zu (1) und (2) sinnvoll eingeschränkt werden. Die aufgezählten Bedrohungen entsprechen dabei denen, die in [BSI05] und [BSI09] genannt werden.

Die Vorschläge und Hinweise (5) werden in Kapitel 3 behandelt. Zu jeder potentiellen Gefahr werden verschiedene Ratschläge unterbreitet. Diese sind mit Markierungen versehen, wodurch sie von einem Programm für bestimmte Sicherheitsbedürfnisse angezeigt werden können. Diese Einteilung geht auf die Schutzstufe und auf das Schutzbedürfnis ein. Die Ratschläge sollen dabei nur einen Einblick geben. Zu jedem Abschnitt ist ein Quelle mit zusätzlichen Informationen genannt.

Die Funktionsweise des Programms (4) wird in Kapitel 4 dargestellt. Für die Datenerhebung werden verschiedene Varianten diskutiert. Anhand eines Beispiels wird die vielversprechendste Möglichkeit simuliert. Dabei wird ersichtlich, wie aus den Bedrohungen (Kapitel 2) und den Maßnahmen (Kapitel 3) ein übersichtliches Programm gestaltet werden kann.

Die abschließende Zusammenfassung (Kapitel 5) enthält sowohl ein Fazit, wie auch einen Ausblick, der auf Hinweise zur praktischen Umsetzung dieses Katalogs aufmerksam macht.

2. Bedrohungsanalyse

In diesem Kapitel wird auf mögliche Bedrohungen eingegangen und eine Übersicht der Gefährdungslage gegeben. Dabei werden die Bedrohungen nach bestimmten Kategorien geordnet und der mögliche Schaden bestimmt. Auch die Eintrittswahrscheinlichkeit wird analysiert. Dabei stützen sich die Ergebnisse auf [BSI05, S. 42ff], wo mehr Informationen über die Details bezogen werden können.

2.1. Übersicht über Bedrohungen einer VoIP-PBX

Eine neue Technologie erweitert meistens auch das Feld der Bedrohungen. Gerade weil diese neue Technologie des Transports von Sprachdaten über verbreitete standardisierte Datennetze abläuft, ergeben sich zahlreiche Bedrohungen gegen VoIP-Systeme. VoIP-Systeme bestehen aus vielen komplexen Einzelkomponenten. Diese können entsprechende Schwachstellen darstellen.

Um Bedrohungen einschätzen zu können, sollten zuerst alle möglichen Angriffspunkte aufgezeigt werden. Die folgende Übersicht gibt eine Einordnung [BSI05, S. 54]:

Unterbindung der Kommunikation

- Störung der Betriebsabläufe (Verfügbarkeit)
- Nichterreichbarkeit der Teilnehmer (Verfügbarkeit)

Umleitung von Datenströmen

- Abhören der Sprachdaten (Integrität, Vertraulichkeit)
- Auslesen von Registrierungsvorgängen an VoIP-Servern bzw. Gateways (Integrität, Authentizität, Vertraulichkeit)
- Manipulation bzw. Modifikation der übertragenen Daten (Integrität, Authentizität, Vertraulichkeit)
- Übernahme von Verbindungen bzw. Sitzungen (Authentizität, Integrität)

2. Bedrohungsanalyse

- Identitätsbetrug (Authentizität, Integrität)
- Verhinderung der Kommunikation (Verfügbarkeit)
- Gebührenbetrug (Authentizität)

Beeinträchtigung der Dienstgüte

- Verzerrung der Sprachkommunikation (schlechte Sprachverständlichkeit, Verfügbarkeit)
- Verlangsamung von Verbindungsauf- und -abbau (Verfügbarkeit)
- Fehlerhafte Gebührenerfassung (Integrität)
- Ausfall einzelner Endgeräte oder Gruppen von Geräten (Verfügbarkeit)

2.2. Bedrohung auf Ebene des Netzwerks

Viele VoIP-Systeme bauen auf Ethernet-Verbindungen, wie sie im LAN¹ bzw. WAN² vorkommen, auf. Daraus ergeben sich alle Bedrohungen von diesen Layern in Verbindung mit den VoIP-spezifischen Bedrohungen. Im Vergleich zur klassischen Telekommunikation ist in einem konvergierenden Netz ein deutlich größerer Personenkreis (Netzwerkadministratoren, externe Dienstleister, Mitarbeiter, Provider) in der Lage, mit einfachen Mitteln (PC, Software) Angriffe auf das LAN auszuüben.

In den folgenden Abschnitten werden die Bedrohungen für das Netzwerk dargestellt. Dabei werden sie nach den verschiedenen Layern des OSI-Modells³ eingeordnet.

2.2.1. Netzwerkinfrastruktur - Bedrohungen von Verkabelungssystemen, Datenverteiltern und Serverräumen

Wie in der Tabelle 2.1 zu sehen ist, gibt es gerade auf der Hardwareebene sehr viele Gefahren für ein Kommunikationssystem. Dabei ähneln diese Gefahren stark denen eines herkömmlichen Telekommunikationssystem. Des Weiteren müssen alle Aspekte der Hardwaresicherung beachtet werden.

Dazu zählen insbesondere die Beschaffenheit der Infrastruktur. Das Gebäude sollte generell gegen höhere Gewalten (Feuer, Blitz und Wasser) geschützt sein. Die schutzbedürftigen Räume sind vor unbefugtem Zutritt, Gefährdung durch Reinigungs-

¹LAN - Local Area Network

²WAN - Wide Area Network

³Open Systems Interconnection Reference Model

2. Bedrohungsanalyse

oder Fremdpersonal, Diebstahl und Vandalismus zu schützen. Die Versorgung durch Strom sollte sichergestellt sein. Mit einem Ausfall der Stromversorgung, mit Spannungsschwankungen, Über- bzw. Unterspannung und Kabelbränden muss gerechnet und eventuelle Vorsichtsmaßnahmen müssen getroffen werden.

Die im System verwendete Hardware kann auch zu Schaden kommen. Es könnten Netzteile durchbrennen, Datenträger defekt werden, Firm- oder Hardwarefehler Ergebnisse verfälschen.

Weiterführende Literatur und Hinweise zu der Infrastruktur gibt es im Grundschutzhandbuch des BSI [[BSI09](#), B 2.1, B 2.2, B 2.4].

Durch die vielen Angriffs- und Ausfallmöglichkeiten auf dieser Netzwerkebene wird die Bedrohung als hoch eingestuft. Das bedeutet nicht, dass von einem Angriff auszugehen ist, sondern der Administrator sollte ein erhöhtes Augenmerk auf diesen Bereich des Systems legen.

Physikalische Ebene

Verkabelungssystem, Datenverteiler und Serverräume

Angriffsmöglichkeiten	Kabeltrassen, Kabelverteilersysteme, Datenverteiler → Durchtrennung der Kabel, Änderungen an Verkabelungsinfrastruktur
	USV-Räume, Leittechnikräume, Klimaräume → Trennung vom Stromnetz, Kurzschluss, Manipulation der Klima-Einstellung
Betroffene Systeme	Es kommt auf die Bereiche an, auf die der Angreifer Zugriff hat. Ist dies eine sehr sensible Stelle (z. B. Serverraum) könnte das gesamte System kompromittiert werden.
Beschreibung	Oftmals stehen Server und Netzwerkkomponenten in unverschlossenen und unüberwachten Räumen. Dadurch wird dem Angreifer neben den oben genannten Möglichkeiten auch der Zugang zur Konsolenschnittstelle der Systeme gegeben.
Fahrlässigkeit	Zugängliche Systeme könnten (z. B. von Reinigungskräften) aus Versehen gestört werden. Je mehr Unbefugte Zutritt haben, desto wahrscheinlicher.
Vorsatz	Der Angreifer kann die Integrität des Systems verändern und dadurch das Telefonsystem außer Betrieb setzen, sich einen unberechtigten Telefonanschluss einrichten, eine Rufumleitung einrichten, Systemeinstellungen löschen oder eigene Software aufspielen, Protokolldaten verändern und andere Manipulationen vornehmen.

Tabelle 2.1.: Bedrohungen physikalische Ebene

2.2.2. Netzwerkebene 2 - Bedrohungen für Switche und VLANs

Die meisten Netzwerke innerhalb eines Unternehmens basieren zur Zeit auf Ethernet-Switches und Routern. In der Vergangenheit setzten viele Firmen diese Art der Infrastruktur ein, da die geschichteten Netze gegenüber Hubs mehr Sicherheit mit sich brachten. Allerdings können die internen Zuordnungen der MAC-Adressen⁴ zu den jeweiligen Ports des Switches durch Angriffe verändert werden. Die Tabelle 2.2 zeigt einige dieser Angriffsmöglichkeiten auf.

Gelingen diese Angriffe, kann es zu unterschiedlichen Auswirkungen führen. In den nicht bedrohlichen Fällen führt es nur zum nicht Erreichen von Servern oder Telefonen. Es könnte allerdings auch ein Man-in-the-middle-Angriff⁵ oder Ähnliches durchgeführt werden. Ein Abhören jeglicher Informationen oder ein Gebührenbetrug wäre somit möglich.

Ein Angriff bzw. eine Störung auf dieser Ebene ist vermutlich nur mutwillig zu erreichen. Der Angreifer muss eine Vorstellung der Anlagen besitzen, die er abhören bzw. unbenutzbar machen will. Der Vorgang des Angriffs wird bei jedem System anders aussehen und kann daher nicht generell automatisiert werden. Die Bedrohung wird als niedrig eingeschätzt.

⁴MAC-Adresse - Media-Access-Control-Adresse

⁵Der Angreifer steht zwischen den Kommunikationspartnern und kann die ausgetauschten Informationen beliebig mithören und verändern ohne bemerkt zu werden

Sicherungsschicht MAC-Adresse, Switches und VLANs	
Angriffsmöglichkeiten	MAC Spoofing → MAC-Tabelle im Switch durch Vortäuschen falscher Adresse verfälschen
	MAC Flooding⁶ → MAC-Tabelle im Switch wird durch hohe Anzahl der gefälschten Anfragen voll und leitet dadurch alle Anfragen an jeden Port
	ARP Spoofing^{7 8} → Gefälschte ARP-Pakete verändern den Empfänger der Pakete
	STP-Attacken⁹ → DoS führt zur Neuberechnung von STP → Durch Fälschung der Kosten kann der Traffic über spezielle Schnittstellen gelenkt werden
	VLAN-Attacken¹⁰ → Kommt ein Angreifer in das VLAN, können alle genannten Attacken auch von extern ausgeführt werden
Betroffene Systeme	Einzelne Telefone, einzelne Server, gesamtes System.
Beschreibung	Gleiche Angriffsmöglichkeiten wie auf andere IP-basierte Systeme
Vorsatz	Der Angreifer kann die Integrität des Systems verändern und dadurch das Telefonsystem oder einen Telefonanschluss außer Betrieb setzen, Gespräche abhören oder Zugangsdaten mitschneiden.

Tabelle 2.2.: Bedrohungen Sicherungsschicht

2.2.3. Netzwerkebene 3 - Bedrohungen für Router und DHCP-Server

Die Netzwerkschicht 3 beinhaltet üblicherweise die Kommunikation mit IP-Adressen. In dynamischen Netzwerken wird die Konfiguration der Routen über DHCP-Server veröffentlicht. Die Kommunikation mit Servern findet meistens außerhalb des Betriebssystemkerns statt und kann somit ohne umfangreiche Programmierkenntnisse erreicht werden.

Durch die Verwendung automatisch zugewiesenen Adressen ist es auch einem Programm möglich, die Angriffe automatisiert durchzuführen. Für Attacken auf verschiedene Systeme kann das Schadprogramm die gleiche Konfiguration nutzen. Außerdem stehen im Internet verschiedene Programmbibliotheken für Angriffe dieser Art zur Verfügung. In einem möglichen Szenario werden die netzinternen Computer benutzt:

Ein Schadprogramm könnte durch ein Virus auf einen Rechner innerhalb des Firmennetzwerkes gebracht werden. Dort übt das Programm den Angriff selbstständig und unentdeckt aus. Danach oder dabei werden sensible Daten auf einen externen Server gesammelt, auf den der Auftraggeber Zugriff hat.

Wählt der Administrator nun statische IP-Adressen und festgelegte Routing-Tabellen, erhöht sich die Konfiguration enorm. Jedes Gerät muss einzeln mit neuen Informationen versorgt werden. Dadurch ist die Wahrscheinlichkeit von Fehlern oder Unvollständigkeit in der Konfiguration deutlich erhöht [Fis08, S. 362f].

Auch andere Szenarien mit DoS- oder auch Man-in-the-Middle-Attacken wären denkbar. Deshalb wird die Bedrohung durch Angriffe auf der Netzwerkschicht 3 mit "hoch" eingestuft.

⁶zu Deutsch: Flut von MAC-Adressen, auch als Switch-Jamming bekannt

⁷ARP - Address Resolution Protocol

⁸zu Deutsch: ARP-Täuschung

⁹STP - Spanning Tree Protocol

¹⁰VLAN - Virtual Local Area Network

Vermittlungsschicht IP-Adresse, Router und DHCP-Server	
Angriffsmöglichkeiten	IP Spoofing → IP-Adresse fälschen um Router oder Firewall zu umgehen
	ICMP Redirect ¹¹ → Netzteilnehmer werden über falsche, angeblich bessere Routen informiert
	IRDP Spoofing bzw HSRP- und VRRP-Angriffe ^{12 13} → Netzteilnehmer wird falscher Gateway mitgeteilt
	Route Injection → In dynamische Routingprotokolle werden fehlerhafte Routen eingeschleust → VoIP-relevante Datenströme werden umgeleitet
	DHCP Starvation → Ständig neue MAC-Adressen führen zur Vergabe aller verfügbaren IP-Adressen
	DHCP Rogue Server → Es wird ein zweiter DHCP-Server an das Netzwerk angeschlossen
	Ping Flood → Ping-Anfragen lasten das Ziel aus und stören es somit bei der Arbeit
Betroffene Systeme	Einzelne Telefone, einzelne Server, gesamtes System.
Beschreibung	Gleiche Angriffsmöglichkeiten wie auf andere IP-basierte Systeme
Vorsatz	Der Angreifer kann die Integrität des Systems verändern und dadurch das Telefonsystem oder einen Telefonanschluss außer Betrieb setzen, Gespräche abhören oder Zugangsdaten mitschneiden.

Tabelle 2.3.: Bedrohungen Vermittlungsschicht

2.2.4. Netzwerkebene 4 - Bedrohungen für Firewall und Protokolle

Die unternehmensinternen Netzwerke werden meist durch geeignete Firewallssysteme von der Außenwelt getrennt. Diese gibt es in den verschiedensten Varianten und Einstellungen. Reagiert die Firewall zu spät auf einen Angriff, könnte das interne Netz bereits beschädigt worden sein. Riegelt die Firewall allerdings die Netze von einander ab, um den Angreifer auszusperrern, können auch alle anderen Dienste nicht mit der Außenwelt kommunizieren. In beiden Fällen wäre mindestens mit einem DoS zu rechnen.

Einige VoIP-Steuerungsprotokolle weisen den Datenströmen bei jeder neuen Verbindung andere Ports zu. Werden diese Protokolle unverschlüsselt übertragen, können Angreifer die neu geöffneten Ports für Angriffe nutzen, bevor die Kommunikation aufgebaut werden kann. Auch andere Schwächen der Protokolle im Bezug auf die Portwahl können ausgenutzt werden.

Da diese Angriffe meist mit sehr viel materiellen Aufwand verbunden sind, ist nicht von einer generellen Bedrohung auszugehen. Erst wenn jemand keine Kosten scheut, wird dieser Angriff, meist durch ein Bot-Netz, durchgeführt.

¹¹ICMP - Internet Control Message Protocol wird verwendet um über bessere oder fehlerhafte Routen zu informieren

¹²IRDP - ICMP Internet Router Discovery Protocol benutzt das ICMP um innerhalb des Netzwerkes andere bzw. bessere Router zu finden

¹³Hot Standby Router Protocol (HSRP) und Virtual Router Redundancy Protocol (VRRP) funktionieren ähnlich wie IRDP

Transportschicht

Angriffsmöglichkeiten	SYN Flood¹⁴ → Viele Verbindungsanfragen überlasten das System → Führt zum DoS
	LAND Flood → System empfängt TCP-Paket mit eigener Absenderadresse → Antwort wird an sich selbst gesendet → Führt zur Auslastung des Systems
	Firewalls und Intrusion Detection Systemen → Durch SYN-Flood-Attacken Port-Filter schließen → Automatische Gegenmaßnahmen des Firewallsystems können für DoS-Angriffe ausgenutzt werden
Betroffene Systeme	Kommunikation zwischen Netzen
Beschreibung	Gleiche Angriffsmöglichkeiten wie auf andere IP-basierte Systeme
Vorsatz	Durch den Angriff können Teile der Infrastruktur von der Außenwelt abgeschlossen werden

Tabelle 2.4.: Bedrohungen Transportschicht

2. Bedrohungsanalyse

2.2.5. Zusammenfassung der Bedrohungen auf Netzwerkebene

In den vorherigen Abschnitten ist detailliert auf die Bedrohungen im Bezug auf das Netzwerk eingegangen worden. In der Tabelle 2.5 sind alle oben genannten Angriffe aufgeführt.

	Datenintegrität	Authentizität	Vertraulichkeit	Verfügbarkeit	Netzwerkschicht
MAC Spoofing		ja	ja		2
MAC Flooding				ja	2
ARP Spoofing	ja	ja	ja	ja	2
STP BPDU-Attacke				ja	2
STP-Umleitung	ja	ja	ja	ja	2
VLAN-Rogue-Trunk	ja	ja	ja	ja	2
VLAN Hopping		ja	ja		2
IP Spoofing		ja	ja	ja	3
ICMP Redirect	ja	ja	ja	ja	3
IRDP Spoofing	ja	ja	ja	ja	3
Route Injection	ja	ja	ja	ja	3
HSRP-Angriffe	ja	ja	ja	ja	3
VRRP-Angriffe	ja	ja	ja	ja	3
DHCP Starvation				ja	3
Rogue-DHCP-Server	ja	ja	ja	ja	3
SYN Flood				ja	4
Land Flood				ja	4
Ping Flood				ja	3
Fragmentierungs Attacken				ja	

Tabelle 2.5.: Übersicht der Netzwerkattacken

¹⁴Client schickt Synchronize-Nachrichten ohne auf die Antwort zu warten

2.3. Bedrohungen durch Gateways und Protokolle

Der Übergang zwischen den herkömmlichen Telefonsystemen und einem VoIP-System stellt aufgrund mehrerer Aspekte ein Sicherheitsrisiko dar. Bei allen Gateways müssen für Signalisierungsvorgänge spezielle Kanäle offen gehalten werden. Diese sind somit auch von außerhalb nutzbar und es können die Schwächen der jeweilig verwendeten Protokolle ausgenutzt werden. Dies ist besonders dann ein Risiko, wenn der Gateway zwei verschiedene IP-Netze miteinander koppelt.

Bei einem Übergang zu einem Telefonnetz gibt es kein Risiko eines Angriffs auf die Signalisierungen von außerhalb. Allerdings werden die meisten Telefonverbindungen im Gegensatz zu VoIP-Verbindungen volumenabhängig abgerechnet. Durch die unberechtigte Nutzung eines Gateways kann es zu einem Gebührenbetrug kommen.

Ein weiteres Problem für den Gateway stellt aber folgendes Szenario dar.

Ein Mitarbeiter möchte nicht gestört werden oder den Administrator nerven. Er programmiert in sein Telefon eine Rufumleitung auf sein Handy. Im Handy schaltet er eine Rufumleitung auf den Apparat im Büro. Erhält der Mitarbeiter nun einen Anruf, werden alle Leitungen im Gateway benutzt und ermöglichen einen DoS [Fis08, S. 365].

Nachfolgend sind die zur Zeit häufig verwendeten Protokolle mit ihren Risiken aufgelistet [BSI05, S. 55]:

RTP¹⁵

- Übertragung der Medienströme von Echtzeitanwendungen
- Sequenznummer, Zeitstempel, Typ, Headerlänge werden übertragen
- durch Vielzahl der Informationen kann durch Kopieren der Pakete alles mitgehört werden

SRTP¹⁶

- RTP mit symmetrischen Schlüssel
- Ohne Kenntnis des Schlüssels kein Abhören möglich
- gilt als sicher

¹⁵RTP - Real-Time Transport Protocol (RFC 3550)

¹⁶SRTP - Secure Real-Time Transport Protocol (RFC 3711)

2. Bedrohungsanalyse

H.323¹⁷

- Authentifizierung werden ohne Verschlüsselung übertragen
- Transportadressen können bei Verbindungsaufbau verändert werden
- Manipulation der Nachrichten durch Man-in-the-Middle-Attacken möglich

SIP¹⁸

- Möglichkeit der Sicherung von Nachrichten durch Hashes
- nicht alle Headernachrichten haben Hashes

MGCP¹⁹ und Megaco²⁰

- Protokolle für die Kommunikation zwischen VoIP-Servern und Gateways
- keine kryptographische Sicherung vorgesehen

Skinny Client Control Protocol (SCCP)

- proprietäres Kommunikationsprotokoll zwischen IP-Telefonen und dem Gatekeeper
- alte Versionen nutzen nur MAC-Adresse zur Authentifizierung
- neue Versionen nutzen X.509 und verschlüsselten Signalisierungsstrom
- weitere Kommunikationen sind unverschlüsselt

2.4. Risiken durch Betriebssystem

Eine sehr wichtige Rolle im Betrieb einer Telefonanlage spielt das zugrunde liegende Betriebssystem (OS, Operating System), welches die Vorgänge der Hardware verwaltet. Bis in die 90er Jahre wurden für die Telefonanlagen noch jeweils eigene Betriebssysteme geschrieben [Fis08, S. 312f]. Danach kamen spezielle Anpassungen von Unix-Derivaten auf den Markt, die den Herstellern die Grundeigenschaften des Betriebssystems abnahmen. Die Treiber für die spezielle Hardware mussten aber auch dafür immer wieder an den OS-Kern angepasst werden.

Circa ab dem Jahr 2000 wurden dann gehärtete Standardbetriebssysteme in den Anlagen eingesetzt. Dadurch werden wertvolle Ressourcen in der Entwicklung eingespart. "Gehärtet" heißt in diesem Falle, dass alle unnötigen Funktionen aus dem

¹⁷H.323 - H.-Standard zur Kommunikation über öffentliche Telefonnetze und ISDN

¹⁸SIP - Session Initiation Protocol (RFC 3261)

¹⁹MGCP - Media-Gateway-Control-Protokoll (RFC 2705)

²⁰Megaco - Media Gateway Control Protocol (RFC 3525)

2. Bedrohungsanalyse

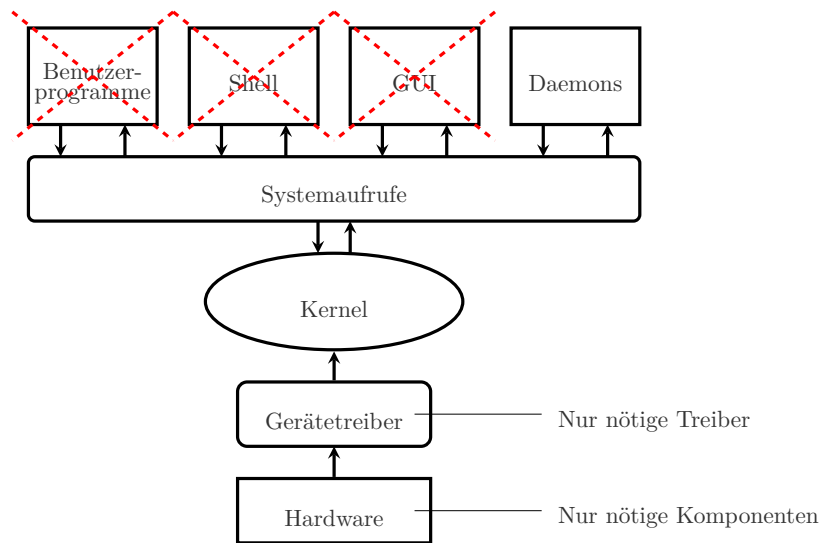


Abbildung 2.1.: Skizze eines gehärteten Betriebssystems mit entfernten Komponenten

Kern entfernt werden. Dies beinhaltet unnötige Treiber und Werkzeuge. Seit 2005 wird zunehmend nur noch Linux wegen der hohen Treiberverfügbarkeit und Betriebsstabilität eingesetzt.

Da Telefonanlagen meistens als geschlossene Einheiten eingesetzt werden, wird meistens auf eine automatische Update-Funktion verzichtet. Wird also in einer Linux-Kernel-Version ein kritischer Fehler entdeckt und behoben, muss der Betreiber einer Telefonanlage selber für die Beseitigung der eventuellen Schwachstelle sorgen. Somit sind alle modernen Telefonanlagen nur so sicher, wie das Betriebssystem die Sicherheit vorgibt.

2.5. Risiken im Bezug auf Hardware

Genauso wie bei den Betriebssystemen (siehe Kapitel 2.4) wandelten sich auch die eingebauten Hardwarekomponenten einer Telefonanlage [Fis08, S. 313ff]. In der Zeit der eigenen OS wurde auch eigene Hardware verbaut, die durch die geringe Stückzahl sehr teuer war. Um Redundanz zu schaffen, wurden dann einige Hardwarekomponenten doppelt verbaut. Eine komplette redundante Telefonanlage war durch die leitungsvermittelten Netze und der direkt einprogrammierten Steuerungen nur sehr aufwendig möglich.

2. Bedrohungsanalyse

Zur Zeit setzt man innerhalb der Anlagen auf Hardware von der Stange mit teilweise mehreren Hardwarekomponenten. Dadurch wird eine einzelne Telefonanlage sehr billig und kann mit einem “normalen” OS verwendet werden. Das gesamte System wird dann (zum Teil sogar räumlich getrennt) redundant betrieben. Bei einem Ausfall eines Systems wird das andere automatisch gestartet, die IP-Pakete werden anders geroutet und somit fällt leitungstechnisch gesehen kein Problem an. Auch die Einstellungen können über die Netze leicht gesichert und auf Backup-Systeme übertragen werden.

Einen weiteren Schritt um die Sicherung der Hardware vorzunehmen, ist der Betrieb innerhalb von virtuellen Maschinen [Fis08, S. 318]. Allerdings gibt es zu dem Betrieb innerhalb dieser wenig Literatur, weil die Versuche dazu noch relativ jung sind [BSI05, S. 61f].

2.6. Bedrohungen auf Anwendungsebene

2.6.1. Programme mit Schadensfunktion

Die Anwendung bezeichnet hierbei die Implementierung der VoIP-Software in den Servern und in den Clients. Dabei kann es zu unterschiedlichen Risiken kommen, die nachfolgend aufgeführt sind. In der Praxis treten auch Mischformen auf. Gerade Würmer nutzen Implementierungsfehler im Betriebssystem um sich zu verbreiten.

Viren

Computer-Viren sind *nichtselbstständige* Programme. Sie reproduzieren sich selbst, benötigen allerdings ein Wirtsprogramm, an dem sie ihren Code anhängen. Dieses Programm können auch Teile des Betriebssystems sein. Für die Infektion gibt es viele Wege. Durch einen verseuchter USB-Stick oder eine E-Mail mit Anhang kann einem PC ein Virus unbemerkt übertragen werden.

Würmer

Computer-Würmer sind *selbstständige* Programme. Sie versuchen sich zu verbreiten, indem Sie über das Netzwerk Schwachstellen anderer Computer ausnutzen. Die Abgrenzung zu Viren besteht darin, dass ein Wurm versucht eine Zahl von Computern zu infizieren, während ein Virus versucht, Dateien auf einem Computersystem zu infizieren.

Trojanische Pferde

Trojanische Pferde sind scheinbar nützliche Programme, die der Benutzer freiwillig auf das System überträgt und ausführt. Im Hintergrund werden dann Funktionen aktiviert, die zur Manipulation oder Ausspähung und Weiterleitung von vertraulichen Daten, sowie zwecks eines vom Benutzer unkontrollierten Fernzugriffs auf das System eingesetzt werden können. Sie verbreiten sich nicht selbstständig.

Implementierungsfehler

Durch Fehler in der Implementierung können unbeabsichtigt Sicherheitslücken geöffnet und das Schadensrisiko unnötig gesteigert werden. Die dabei am häufigsten ausgenutzten Implementierungsfehler führen zu so genannten Pufferüberlauf-Angriffen (Buffer-Overflow). Diese können zur Übernahme des gesamten Systems führen. Aber auch bei der Implementierung von Netzwerkprotokollen können Fehler aufgrund inkorrekt verarbeiteter Daten entstehen. Ein Absturz des Systems ist somit möglich.

2.6.2. VoIP-Endgeräte

Generell unterscheidet man zwei Arten von Endgeräten: IP-Telefone und Softphones.

IP-Telefone sehen von außen wie herkömmliche Telefone aus und besitzen eine Ethernetbuchse für ein LAN-Kabel. Es sind auch IP-Telefone mit WLAN erhältlich, die wie gebräuchlich schnurlose Telefone aussehen. Sie erhalten meistens ihre Konfigurationen über das Netzwerk. Dafür gibt es Protokolle, wie das TFTP²¹. Auch das Laden des benutzerabhängigen Telefonbuchs kann dynamisch mit der Anmeldung erfolgen.

Softphones sind Programme, die auf PCs installiert werden können. Dabei wird die Netzwerkschnittstelle des Computers für die Kommunikation eingesetzt. Der Funktionsumfang ist bei dieser Variante ähnlich dem reinen IP-Telefon.

Im Bereitschaftsmodus warten Geräte auf Benutzereingaben oder auf die ankommenden Anrufe. Durch die in Kapitel 2.6.1 aufgezeigten Möglichkeiten kann das System infiltriert werden. Folgen wären zum Beispiel: Gebührenbetrug, Abhören der Gespräche, DoS, Ausspähen und Ändern des Telefonbuchs, falsche Weiterleitungen, aber auch die Aktivierung des Mikrofons als Wanze.

²¹Trivial File Transfer Protocol, verbindungsloses Protokoll

2. Bedrohungsanalyse

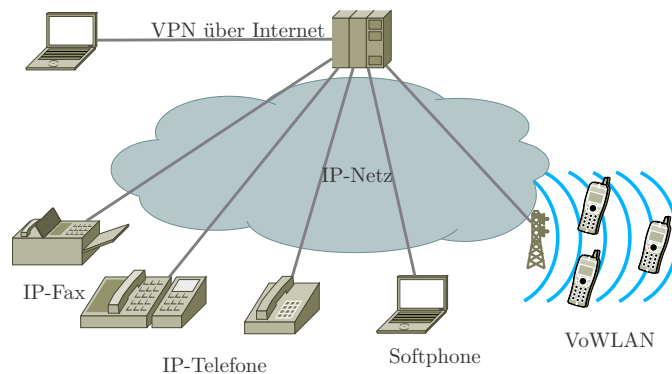


Abbildung 2.2.: Endgeräte im Netzwerk

Die Bedrohung eines Angriffs auf ein IP-Telefon sind bedeutend geringer, als auf ein Softphone. Das IP-Telefon wird meist mit speziell angepasster Hardware und proprietärer Software (Betriebssystem) ausgeliefert. Dadurch ist jeder Angriff mit hohem Aufwand verbunden. Bei den Softphones gibt es viele Möglichkeiten eines Angriffs, denn ein Angriff auf ein verbreitetes Betriebssystem (Windows, Unix, Linux) ist relativ einfach möglich, wie in Kapitel 2.4 gezeigt wird.

2.6.3. VoIP-Middleware

Nachfolgend sind die verschiedenen Server und Software aufgeführt, die bei einer VoIP-Installation benötigt werden. Zu jedem Programm wird kurz die Funktion erklärt und mögliche Risiken genannt.

Zu beachten ist, dass die aufgeführten Server nicht unbedingt physisch getrennt sein müssen. Alle genannten Servern können als Software auf dem gleichen Gerät laufen, wie es bei kleineren Telefonanlagen, wie zum Beispiel der FritzBox, der Fall ist.

Gatekeeper

Gatekeeper (auch Callmanager oder Call-Server genannt) sind Telefonanlagen auf IP-Basis. Diese server-basierten Softwarelösungen sind zuständig für die Signalisierung und Durchführung von Anrufen, Verteilung der Konfiguration für VoIP-Endgeräte, Verwalten von Benutzern, Zugriffskontrolle, sowie zur Verwaltung von Sprachnachrichten (Voice-Mails). Einige Gatekeeper erlauben eine Fernsteuerung über eine Web- oder Konsolenschnittstelle.

2. Bedrohungsanalyse

Die gängigen Gatekeeper werden auf herkömmlichen Betriebssystemen installiert und sind demnach auch den systemspezifischen Angriffen ausgesetzt, wie es in Kapitel 2.4 beschrieben wurde. Erhält der Angreifer Zugriff auf Gatekeeper, könnte dies zahlreiche Folgen auf Authentizität, Integrität, Verfügbarkeit und Vertraulichkeit haben. Die Funktionen von Gatekeeper können zudem durch Angriffe auf seine Untersysteme (Datenbank: SQL-Slammer; Voice-Mail: Spam) gestört werden.

VoIP-Router

VoIP-Routern ähneln in der Funktionalität den Routern in übrigen IP-Netzwerken. Sie leiten VoIP-Pakete in die jeweiligen IP-Subnetze und stellen meist auch Anschlüsse für analoge Telefone bereit. Meistens können Sie über eine Webinterface konfiguriert werden.

Gerade in privaten Haushalten sind diese VoIP-Router zusammen mit einem WLAN-Accesspoint, einem Switch, einem DSL-Modem und einem DSL-Router in einem Gerät integriert. Dieses wird vom Netzbetreiber für den jeweiligen Telefon- und DSL-Vertrag zur Verfügung gestellt. Durch diese weite Verbreitung in privaten Haushalten ist eine große Ausbeute bei Angriffen möglich. Deshalb stellt jedes Gerät, welches auch von Netzbetreibern Kunden zur Verfügung gestellt wird, ein höheres Risiko dar.

VoIP-Gateways

VoIP-Gateways bestehen aus Media-Gateways und Media-Gateway-Controllern. Media-Gateways (MGs) sind Netzwerkkomponenten der VoIP-Infrastruktur, die eingesetzt werden, um leitungsorientierte Verbindungen in IP-basierte Verbindungen zu konvertieren um Kosten zu sparen. Diese können von Media-Gateway-Controllern (MGCs) ferngesteuert werden. Die Übernahme eines solchen MGCs ermöglicht den Angreifern den vollen Zugriff auf alle angeschlossenen MGs. Viren oder Ähnliches können allerdings nicht über die leitungsorientierten Anschlüsse verbreitet werden.

VoIP-Firewalls

Firewalls werden eingesetzt, um vor Angriffen und unerlaubtem Zugriff zu schützen. Die Pakete werden von Firewalls mit den Filterregeln geprüft und dann weitergeleitet. Sie können auf proprietären und üblichen Betriebssystemen installiert und meistens mit einer geeigneten Schnittstelle bedient werden.

2. Bedrohungsanalyse

In VoIP-Netzwerken kann die Firewall anhand der Paketheader zwischen den verschiedenen Protokollen unterscheiden. Es kontrolliert, ob in der jeweiligen Phase des Gesprächs diese Pakete laut Protokoll ausgetauscht werden dürfen. Gelingt es einem Angreifer Kontrolle über die Firewall zu erlangen, kann er die Gesprächsvorgänge beeinflussen (z. B. stören, umleiten, abhören). Es ist auch wichtig darauf zu achten, dass Anhänge einer Voice-Mail Viren enthalten können.

Zusammenfassung zur Bedrohung der VoIP-Middleware

Bei Angriffen auf VoIP-Middleware können alle dadurch geleiteten IP-Telefonate gestört, abgehört, umgeleitet und manipuliert werden. Anders als bei Angriffen auf die Endgeräte (Kapitel 2.6.2) haben diese Systeme ein höheres Risiko im Bezug auf die Sicherheit. Wichtig wäre deshalb die Sprach- und Datenpakete physisch zu trennen. Außerdem wird ein Großteil der Angriffe auf die Schnittstellen zur Konfiguration angesetzt. Deshalb sollte generell in Frage gestellt werden, ob eine Fernwartung notwendig ist. In jedem Fall ist die Sicherheit nur so hoch, wie ihr schwächstes Glied.

2.6.4. WLAN

Als besonders wichtiger sicherheitskritischer Punkt sollte das WLAN angesehen werden. Mit Hilfe des WLANs kann die Netzwerkinfrastruktur kostengünstig erweitert werden. Es ermöglicht ein Telefonieren mit VoWLAN-Geräten (Voice-over-WLAN). Diese Geräte sind VoIP-Telefone, die direkt über WLAN kommunizieren.

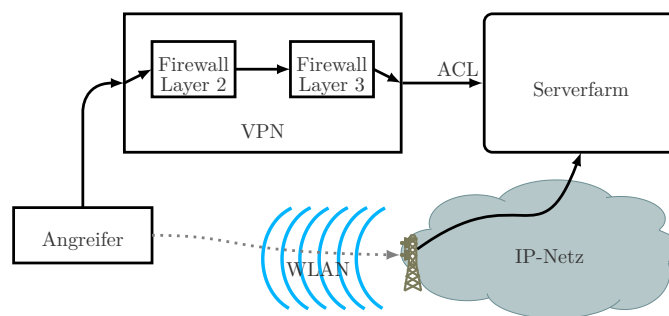


Abbildung 2.3.: Angriff über WLAN ist meist viel einfacher

Durch WLAN ist es Angreifern möglich viele Sicherheitsvorrichtungen zu überspringen und direkt Angriffe auf die VoIP-Infrastruktur zu starten. Sicherungen im Bereich der Netzwerkebene (Kapitel 2.2) und mittels Firewalls (Kapitel 2.6.3) können umgangen werden, wenn der Angreifer sich Zugang zum WLAN verschaffen kann.

2. Bedrohungsanalyse

Angriffsmöglichkeiten für WLAN gibt es sehr viele. Durch die Anzahl der Varianten der Standards und Verschlüsselungen ist eine ausführliche Betrachtung dieser Bedrohungen im Rahmen dieser Arbeit nicht möglich. An dieser Stelle sei auf weiterführende Literatur, wie [BSI05, S. 65ff], [Fis08, S. 102ff] und [BSI09, B 4.6] verwiesen.

3. Sicherheitsmaßnahmen

In den folgenden Abschnitten werden Sicherheitsmaßnahmen für die Installation von VoIP-Anlagen genannt. Tiefgreifendere Informationen dazu befinden sich in [BSI05, S. 71ff] und [BSI09, M 5, B 4.7]. Zu jedem Abschnitt wird kurz erklärt, welche Bedrohungen abgedeckt werden sollen.

Die Maßnahmen sind mit Hinweisen versehen, die anzeigen, bei welchen Schutzbedürfnissen sie angewandt werden sollen. Es wird hierbei mit Abkürzungen gearbeitet, die für folgende Bedürfnisse stehen:

<i>F</i>	Verfügbarkeit
<i>I</i>	Integrität
<i>A</i>	Authentizität
<i>T</i>	Vertraulichkeit
+	Erhöhte Schutzbedürfnis

Tabelle 3.1.: Abkürzungen der Schutzbedürfnisse

Das ‘+’ an einem Buchstaben weist darauf hin, dass diese Maßnahme nur nötig ist, wenn es dieses Bedürfnis besonders zu schützen gilt. Des Weiteren wird eine Zahl über die Sicherheitseinstufung Auskunft geben. Eine Maßnahme mit Einstufung ‘1’ sollte bei jeder Installation beachtet werden. Die Maßnahmen mit Einstufung ‘5’ sind nur für besonders zu schützende Installationen notwendig. Eine Einstufung der Maßnahmen für eine automatische Auswertung ist somit gegeben.

Als Beispiel wird eine Seelsorgehotline mit VoIP ausgestattet. Um bei einer solchen Hotline anzurufen muss man ein hohes Maß an Vertrauen besitzen. Die Verfügbarkeit ist aber nicht besonders wichtig. Mit Gebührenbetrug oder Angriffen ist nicht zu rechnen. Aus diesen Tatsachen kann man eine Einstufung in ‘I,T+,3’ wählen.

3. Sicherheitsmaßnahmen

3.1. Sicherheit der Netzstruktur und ihre Komponenten

Die Maßnahmen für den Bereich der Netzstruktur sind nach den Layern des OSI-Modells geordnet. Im Abschnitt 2.2 werden die zugehörigen Bedrohungen aufgelistet.

3.1.1. Layer 1

Physikalischer Schutz

- getrennte, verschließbare und überwachte Serverräume ($I, A, T+, 3$)
- physikalischer Zutritt sollte nur autorisierten Personen erlaubt sein ($F, T, 3$)
- Zutrittskontrolle über Smartcards oder Einmal-Passwörter und Videoüberwachung ($T, 4$)
- Sicherungsmaßnahmen der Räume gegen Stromausfall, Wasserschaden und Feuer erhöhen ($F, 3$)
- Kabeltrassen durch Verkleidung oder Unterputzverlegung schützen ($F, I, 4$)

Stromversorgung

- Power-over-Ethernet (PoE): Möglichkeit, die Stromversorgung zentral über das Ethernetkabel zu leiten¹ ($F, 4$)
- Unterbrechungsfreie Stromversorgung (USV)
 - Middleware wird korrekt heruntergefahren ($F, 3$)
 - Aggregate zur dauerhaften Versorgung ($F+, 5$)
 - Benachrichtigung durch SMS/E-Mail/Pieper ($F, 4$)

Trennung von Sprach- und Datennetz

- physikalische Trennung ($I, A+, V+, 5$)
- logische Trennung
 - VLAN mit geeigneten Switches ($A, T, 3$)
 - MAC-Adressenzuweisung zu Ports ($A, 2$)
 - Authentisierung nach 802.1x ($A+, 4$)

¹Nur in Verbindung mit USV sinnvoll, die das Ethernetkabel mit Strom versorgt

3. Sicherheitsmaßnahmen

3.1.2. Layer 2

Authentifizierung Endgeräte

- VLAN-Authentisierung
 - MAC-Adressenzuweisung zu Ports ($A, 2$)
 - Authentisierung nach 802.1x ($A+, 4$)
- in Endgeräte eingebaute Switches deaktivieren bzw. keine Switches hinter den Anschlussdosen erlauben ($A, 3$)
- externe Nutzer (Heimarbeitsplätze) nur mit VPN und Firewall ($A, I+, T+, 2$)

MAC Spoofing

- statische MAC-Einträge (mindestens für Middleware) ($A, 2$)
- Aktivierungszeiten am Switch-Port festlegen ($A+, 3$)
- Verletzungslimitierung einschalten ($A+, 4$)
- 802.1x Authentifizierung ($A+, 4$)

ARP Spoofing

- Gratuitous-ARP abschalten (verhindert das ungeprüfte Übernehmen von Broadcastmeldungen) ($I, A, T, 3$)
- statische ARP-Einstellungen vermeiden (diese werden meistens überschrieben) ($A, 3$)
- Proxy-ARP abschalten ($A, 3$)

DHCP-Attacken

- gegen DHCP-Starvation gibt es Optionen im Switch oder explizite Konfigurationen ($A, 3$)
- um Rogue-Server abzuwehren, gibt es Filteroptionen in moderneren Switches ($A, 4$)

Anti-Spoofing-Filter

- Anti-Spoofing-Filter prüfen externen Verkehr auf gültige Quelladressen ($A+, 4$)
- sollten immer allen anderen internen und externen Netzfilterregeln vorangestellt werden ($I, A, T, 3$)

3. Sicherheitsmaßnahmen

VLAN-Angriffe

- native Tunnel gegen VLAN-Hopping ($I+$, 4)
- Untersuchung der Ethernet-Frames mit VLAN-ACLs in Switches und ACLs in Routern ($I+$, 5)
- Port-basierende ACLs auf dem Promiscuous-Port der Switches ($I+$, 5)

Netzzugang aus dem öffentlichen Netz ins LAN

- VPN-Verbindungen mit einer Authentifizierung und Verschlüsselung ist eine Voraussetzung ($I, A, T, 2$)
- Zugang durch spezielle Firewall gesichert ($A, 2$)

3.1.3. Layer 3

Alle folgenden Maßnahmen sind für I, A, T wichtig.

- Anti-Spoofing-Filter in den Routern (gegen IP-Spoofing) (3)
- Verarbeitung von Redirect-Nachrichten abschalten (gegen ICMP-Redirect) (3)
- IRDP sollte man nicht einsetzen (gegen IRDP-Spoofing) (3)
- Zugriffslisten auf allen Ports bzw. Netzübergängen konfigurieren, über die keine Routingprotokollnachrichten gesendet werden dürfen (gegen Route-Injection) (4)
- Firewall zum Schutz vor Massenanfragen (Ping Flood, SYN Flood und LAND Flood), allerdings muss Firewall auch durch IDS-System² geschützt werden (3)

3.1.4. Redundante Komponenten

Redundanzkonzepte sind in der Absicherung eines Netzwerkbetriebes sehr wichtig, wenn man annähernd die gleiche Verfügbarkeit des VoIP im Vergleich zu der herkömmlichen Telefonie erreichen will. Die einzusetzenden Dienste müssen im Hot-Standby³ laufen und sich je nach Aufgabe automatisch einschalten. Die nachfolgenden System sind nach aufsteigender Umschaltzeit geordnet. (F)

Generell sollten ab Stufe (2) alle Hardwarekomponenten redundant verfügbar und in wichtigeren Stufen im Hot-Standby angeschlossen sein.

²IDS - Intrusion Detection System, System zur Erkennung von Angriffen

³Hot-Standby, oder Failover bezeichnet den ungeplanten Wechsel von Serverkomponenten

3. Sicherheitsmaßnahmen

DHCP-Server, TFTP-Server, FTP-Server

Da Telefone ihre Konfigurationen nur alle 3-6 Stunden erneuern, reicht eine Umschaltzeit im Minutenbereich aus. Falls die Telefone keine Dienste erreichen, löschen sie normalerweise die alten Konfigurationen nicht. (3)

Registrars, Gatekeeper oder Call Manager

Eine Umschaltung im Sekundenbereich ist notwendig, weil diese Systeme die Berechtigungen jedes aufzubauenden Anrufs kontrollieren. Notrufe sollten ohne Berechtigung möglich (Notrufe, siehe Abschnitt 3.3) und die Datenbank für dieses System dementsprechend verteilt sein. (3)

Provisioning-Server

Diese dienen zur Gebührenabrechnung. Auf die Abrechnung kann einige Sekunden verzichtet werden. (4)

Firewall

Wenn auch die Medienströme durch die Firewall geleitet werden, ist eine Umschaltzeit unter einer Sekunde nötig, um die laufenden Verbindungen nicht zu unterbrechen. (3)

Switches und Router

Grundsätzlich gibt es zwei Strategien zur Anbindung an das Netz. Im ersten Fall werden zwei gänzlich getrennte Service-Areas betrieben. Dabei sind keine besonderen Vorkehrungen zu treffen. Im zweiten Fall kann Spanning-Tree oder Fast-Spanning-Tree zur Umschaltung eingesetzt werden, wodurch teilweise kostspielige Hardware gespart werden kann. Die Umschaltzeiten sollten sich auch hierbei unter einer Sekunde befinden, um die laufenden Verbindungen nicht zu unterbrechen. (3)

3. Sicherheitsmaßnahmen

VoIP-Gateway

ISDN-Verbindungen sehen keinen Mechanismus für eine Umstellung eines laufenden Systems vor. Fällt hier also ein Bauteil oder eine Verbindung aus, müssen die anderen Gateways für die Verbindungen sorgen. Generell sollte eine Gleichverteilung unter den Gateways stattfinden, um im Fehlerfall nur eine kleine Anzahl von Gesprächen zu unterbrechen. (4)

3.2. Dienstgüte und Netzmanagement

Es werden in der Literatur verschiedene Ansätze aufgeführt, wie man die Dienstgüte innerhalb eines Netzwerkes garantieren kann. Dabei können die Ansätze auch kombiniert werden. Nachfolgend werden diese Ansätze nur kurz genannt, da eine ausführliche Beschreibung den Rahmen dieser Arbeit überschreiten würde.

Generell kann gesagt werden, dass ab Stufe (3) über die Dienstgüte nachgedacht werden sollte. Vorhandene Strukturen sollten erweitert und an die VoIP-Umgebung angepasst werden.

Differentiated Services (DiffServ)

Ein Schema⁴ zur Klassifizierung von IP-Paketen, die ein Bevorzugen von bestimmten Datenpaketen erlaubt. Dadurch können Mediendaten schneller geroutet werden. Andere Daten müssen warten. Dabei ist sehr wichtig, dass alle Daten die richtigen Markierungen aufweisen.

Overprovisioning

Beim Overprovisioning werden alle Netzkomponenten gezielt über proportioniert. Durch permanentes Monitoring werden potentielle Engpässe aufgezeigt und behoben. Gerade die CPU-Auslastung der Middleware kann zu Engpässen führen. Ein Overprovisioning garantiert allerdings kein QoS, sondern baut nur auf Statistiken auf.

⁴DiffServ wird in RFC 2474 spezifiziert

3. Sicherheitsmaßnahmen

MPLS

Mittels Multiprotocol Label Switching (MPLS⁵) kann eine garantierte Durchsatzrate über lange Strecken ermöglicht werden. Die Adressierung der Pakete wird dabei vereinfacht und ermöglicht eine virtuelle verbindungsorientierte Übermittlung.

Traffic Shaping

Traffic Shaping wird in Gateways eingesetzt, um die Datenraten bestimmter Anwendungen zu drosseln. Dabei werden Datenströme an bestimmte Ports durch Filter überwacht. Sie können aber leicht umgangen werden und garantieren keinen QoS.

Störungsmanagement, Eskalationsprozesse und Security Management

Um einen Ausfall bei Störungen vorzubeugen und im Ernstfall schnell beheben zu können, sollten ein Störungsmanagement eingerichtet werden. Die Eskalationsprozesse sollten definiert werden. Baugleiche Hardware oder Ähnliches sollte als Notreserve vorhanden sein. Im Security-Management-Katalog sollten alle Maßnahmen festgehalten werden, damit auch bei einem möglichen Personalausfall eine Störung beseitigt werden kann.

3.3. Besondere Maßnahmen für Notrufe

*Wer öffentlich zugängliche Telefondienste erbringt, ist verpflichtet, für jeden Nutzer unentgeltlich Notrufmöglichkeiten unter der europaeinheitlichen Notrufnummer 112 [...] bereitzustellen.*⁶

Weiterhin heißt es im Gesetz, dass es jedes Telekommunikationsgerät, das sichtbar im Betrieb ist, einen Notruf absetzen können muss. Daten für Standortbestimmungen und gegen Missbrauch müssen übermittelt werden. Außerdem muss die richtige Leitstelle angerufen werden. Diese Bestimmungen stellen die VoIP-Installationen vor Herausforderungen, die gemeistert werden müssen um den deutschen Gesetzen zu entsprechen [Fis08, S. 288ff].

⁵RFC 3031 spezifiziert MPLS Architecture

⁶Telekommunikationsgesetz §108 "Notruf" Absatz 1, Satz 1

3. Sicherheitsmaßnahmen

Die dynamische Architektur des IP-Netzes vermindert die genaue Standortkontrolle des Endgerätes. Deswegen muss der Gateway immer eine Möglichkeit haben, zu erfahren wo sich das Telefon befindet. Dies kann man mit speziellen Netzwerkmanagement erreichen. Im WLAN wird die Kontrolle komplizierter. Normalerweise reicht aber hier die Lage des jeweiligen Accesspoints für die Standortbestimmung aus.

Die Zentralisierung der Server ist für die Standortbestimmung ein weiteres Problem. Verschiedene Firmensitze besitzen heutzutage nur eine zentrale VoIP-Infrastruktur. Der Anruf wird also zuerst von dem Außensitz zur Zentrale geroutet und muss nun an die richtige Leitstelle zurückgesandt werden. Das gleiche Problem tritt bei Internettelefonie auf.

Für all diese Fälle ist ein besonderes Konzept zu erarbeiten. Zur Not sollte auf jeden Fall eine GSM-Schnittstelle zusätzlich zu anderen Gateways für den Notruf integriert werden (3).

Beispielkonfiguration mit AAA-Server

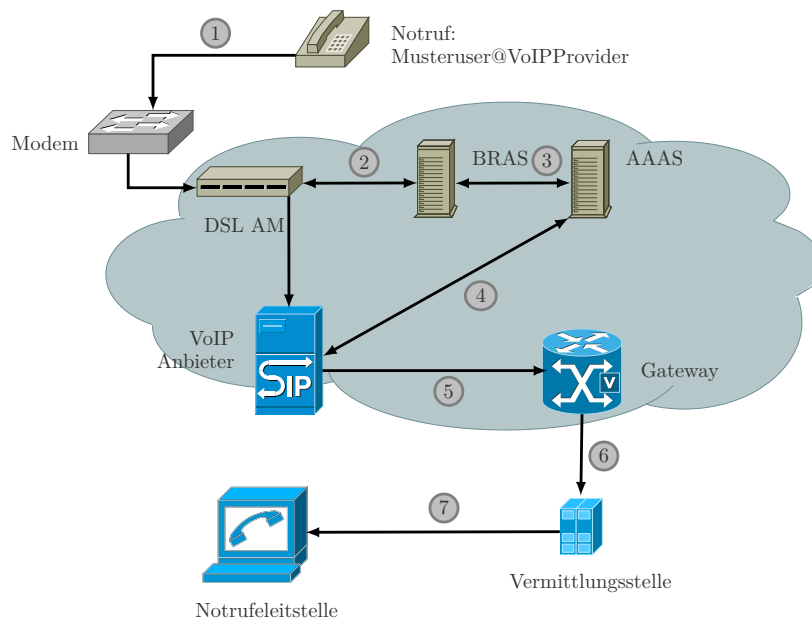


Abbildung 3.1.: Beispiel für die Absetzung eines Notrufs

Für Nutzer eines DSL-Anschlusses und einem VoIP-Anbieter im Internet gibt es einen vielversprechenden Ansatz. Dem Netzbetreiber ist der Standort des Teilnehmers bekannt, denn er kann über den jeweiligen Port des DSL AM⁷ eindeutig ein

⁷DSL AM - Digital Subscriber Line Access Multiplexer

3. Sicherheitsmaßnahmen

Gebäude oder sogar eine Etage bestimmen. Bei jeder Anmeldung wählt sich der Benutzer im BRAS⁸ ein und erhält eine dynamische IP-Adresse. Ein AAA-System⁹ identifiziert den Benutzer dabei. Alle nötigen Informationen sind vorhanden, sie müssen nur bei einem Notruf abgefragt werden können.

In Abbildung 3.1¹⁰ ist der Ablauf eines Notrufs dargestellt.

1. der DSL AM registriert eine Einwahl und setzt den Port vom Benutzer *Musteruser* mit der jeweiligen Adresse¹¹ gleich.
2. bei der Anmeldung am BRAS bekommt der Nutzer eine IP-Adresse zugewiesen
3. er Authentifiziert sich am Triple-A-System, welches nun auch die IP-Adresse, den DSL AM-Port speichert
4. im Falle des Notrufs fragt der VoIP-Anbieter das Triple-A-System nach den Informationen
5. über einen Gateway wird die zu dem Standort passende Leitstelle angewählt
6. eine PSTN leitet die Verbindung auf herkömmliche Weise zur Notrufabfragestelle

3.4. Aspekte im Zusammenhang mit Protokollen

Störungen der Anwendung (DoS) und der Basisdienste

- einspielen von Sicherheits-Patches für alle Komponenten (1)
- Abschaltung aller nicht nötigen Dienste (2)
- Fernzugriff nur über verschlüsselte Verbindungen (SSH, HTTPS), hierauf ist schon beim Kauf der Systeme zu achten (2)

⁸BRAS - Broadband Remote Access Server

⁹AAA - Authentication, Authorization, Accounting

¹⁰http://www.voip-info.de/wissen/_Artikel_Allgemein_2011.php?page=3

¹¹Je nach Gebiet kann die Adresse eine Straße, eine Hausnummer, eine Etage oder sogar genau ein Netzabschluss sein

3. Sicherheitsmaßnahmen

Abhören und Manipulation von Medienströmen

- RTP-Daten nur über eine verschlüsselte Verbindung (IPsec¹², PPTP¹³, TLS/SSL¹⁴) übertragen (2)
- SRTP verschlüsselt nur die Sprachinformationen, spezielle Endgeräte benötigt (2)
- Protokolle H.323, SIP und SCCP unterstützen Methoden zum Schlüsselaustausch für SRTP (2)

Manipulation der Signalisierung und Gebührenbetrug

Die folgende Auflistung sollte nur entsprechend der gewählten Protokolle angezeigt werden. Sie wird erst ab Stufe (3) benötigt. Es besteht eine Ausnahme, wenn (A+) gefordert ist.

- Protokolle MGCP und Megaco
 - verschlüsselte VPN-Kanäle sollten eingerichtet werden
- H.235
 - Möglichkeit zur Integritätsüberprüfung und Verschlüsselung der Signalisierung nach H.323
 - Schlüsselverwaltung auf X509-Zertifikate-Basis
- Session Initiation Protocol (SIP)
 - sichere Übertragung der Passwörter zur Authentifizierung gegeben
 - einige Header-Felder sind durch Signatur geschützt
 - gesamtes Paket kann nicht signiert werden, weil Header durch SIP-Proxy verändert wird
 - Identitätsbetrug durch falsche Absenderkennung möglich
- SIP über TLS
 - Verbindung komplett verschlüsselt
 - Nachrichten werden über TCP statt UDP ausgetauscht

¹²IPsec - Internet Protocol Security, RFC 4301

¹³PPTP - Point-to-Point Tunneling Protocol, RFC 2637

¹⁴Transport Layer Security (TLS), ehemals Secure Sockets Layer (SSL), neuester RFC ist 4346

3.5. Firewalls und NIDS zur Sicherung des Netzwerkes nach außen

Anforderungen an eine Firewall

- Sicherheitsrichtlinien (Security Policy) definieren und mit Firewall umsetzen (3)
- VoIP-fähige Firewall verwenden (Signalisierungsprotokolle mit dem gesamten Rufauf- und -abbau analysieren und in den jeweiligen Zustände die Ports freischalten) (A, 4)
- Leistung der Firewall wirkt sich auf Delay und Jitter aus (I, 2)

Paketfilter auf Layer 3 und Layer 4 (Stateless Packet Filter)

- Filter für einzelne Pakete definieren (4)
- erhebliche Einschränkung gegenüber zustandsbasierten Portfiltern beachten (3)

Zustandsbasierende Portfilter auf Layer 3 und Layer 4 (Stateful Packet Inspection)

Im Vergleich zu den zustandslosen sollten die zustandsbasierte Portfilter verwendet werden, weil

- Ports für Rückpakete dynamisch geöffnet werden und (4)
- die Zustände der Kommunikation gespeichert werden (4)

Application Level Gateway (ALG)

- meistens eingebettete Software, die Parser für H.323, SIP, MGCP und SDP¹⁵ bereitstellt (4)
- Ports werden dynamisch geöffnet (4)
- Zustände werden gespeichert und kontrolliert (4)
- die bei RTP ständig wechselnden UDP-Ports werden dynamisch geöffnet (4)

Network Intrusion Detection System (NIDS)

- prüft Netzwerkverkehr mit Angriffsmuster, die vorher definiert wurden (4)
- analysiert Verkehr mit Heuristik um Angriffe zu erkennen (4)

¹⁵SDP - Session Description Protocol, RFC 4566

3.6. Maßnahmen für VoIP-Komponenten im Netzwerk

3.6.1. Middleware

Die Bedrohungen für die Middleware wurden bereits in Abschnitt 2.6.3 aufgeführt. Generell gelten folgende Maßnahmen:

- nicht genutzte Dienste abschalten (2)
- Administration und Konfiguration nur über gesicherte Verbindungen (SSH, HTTPS) durchführen (2)
- Konfigurationen für verschiedene Middleware physisch voneinander trennen (3)
- Berechtigungsstufen und Administrierkonzept festlegen (3)
- regelmäßige Datensicherungen durchführen(2)
- eingesetzte Software ist auf dem aktuellen Stand halten (1)
- eingesetzte Betriebssysteme härten (2)

3.6.2. Endgeräte

Generell gelten hier die identischen Maßnahmen, welche auch für die Middleware (Abschnitt 3.6.1) eingesetzt werden. Zusätzlich ist Folgendes zu beachten:

- Firmware-Updates nur über gesicherte Verbindung durchführen(1)
- lokale Konfiguration deaktivieren, wenn automatische Konfiguration eingesetzt wird (3)
- Zertifikate der Konfigurationsserver installieren (2)
- Personenbezogene Zugangskontrolle durch Passwörter oder Smartcards festlegen (3)
- angeblich implementierte Sicherheitsmaßnahmen überprüfen (4)

3.7. Protokolle

Steuerinformationen und Mediendaten werden in den gängigen Protokollen von einander getrennt übertragen. Zu den Steuerinformationen gehören Zustände wie "besetzt" oder der Authentifizierungsvorgang. Außerdem wird der Medienaustausch organisiert. Die meist unterstützten Medien sind: Sprache, Video und Fax.

Die Protokolle sind untereinander nicht kompatibel. Deswegen sollte schon im Vorfeld darauf geachtet werden, dass Middleware und Endgeräte die gleichen Protokolle benutzen. Durch einen Gateway wäre es theoretisch möglich, die unterschiedlichen

3. Sicherheitsmaßnahmen

Architekturen miteinander zu verbinden. Allerdings stellt ein solcher Gateway dem Netz neue Angriffsmöglichkeiten zur Verfügung.

Gerade die zentrale Middleware bestimmt die Wahl der Protokolle. Diese Geräte bilden meist den kostenintensiveren Teil der Hardware und können somit schwieriger ausgetauscht werden. Im folgenden sind die Protokolle SIP und H.323 erläutert, da sie zur Zeit die häufigste Verwendung finden. Für weitere Informationen sollte [BSI05, S. 101ff] und [BSI09, M 5.133] dienen, wo auch zusätzliche Protokolle aufgelistet sind.

3.7.1. Session Initiation Protocol (SIP)

- spezifiziert in RFC 3261
- Verschlüsselung durch SSL bzw. TLS oder IPSec
- Sprachinformationen über RTP
- Adressschema: *Benutzer@Domain*
- Auflösung der Domain über DNS (*A*)
- Ähnlichkeit mit dem HTTP-Protokoll, deshalb einfach verständlich
- Standard, an den sich einige Hersteller nicht halten (*F*)

Beteiligte Komponenten

- Endgeräte (Telefon, Softphone, Gateway)
- Location Server (liefert die IP-Adresse zu Benutzernamen)
- Registrar (Anmeldung und Registrierung)
- SIP-Proxy (Rolle des Vermittlers)

3.7.2. H.323

- ursprüngliche Umsetzung für ISDN-D-Kanal
- beschreibt den Rahmen für
 - H.225.0 (Signalisierung)
 - H.245 (Kontrolle der Sprachinformationen)
 - H.450 (Telefoniefunktion)
 - H.235 (optional) (*I, T*)
- Audio- und Videodaten per UDP
- Faxdaten per UDP oder TCP
- Übertragung der Medieninformationen über logische RTP und RTCP-Kanäle
- Nachteil durch enorme Komplexität des Protokolls

3. Sicherheitsmaßnahmen

Beteiligte Komponenten

- Terminals (Endgeräte)
- Gatekeeper (Verwaltung, Steuerung)
- Multipoint Control Unit (optional für Konferenzen)
- Gateways (Übergang zu anderen Netzen)

4. Expertensystem

In den vorherigen Kapiteln wurden die Bedrohungen (Kapitel 2) und dazu erforderlichen Sicherheitsmaßnahmen (Kapitel 3) für eine VoIP-Umgebung zusammengetragen. In den folgenden Abschnitten wird aus den gesammelten Informationen ein Programm zur automatischen Entscheidungsempfehlung entwickelt. Eine solche Software wird auch als Expertensystem bezeichnet.

4.1. Allgemeiner Ablauf des Programms

Im Grunde soll das Programm dazu dienen, dass Netzwerkadministratoren oder andere, an der Sicherheit von VoIP-Installationen interessierte Personen, relativ einfach Ratschläge und Maßnahmen aufgezeigt werden. In Abbildung 4.1 ist der allgemeine Ablauf dargestellt.

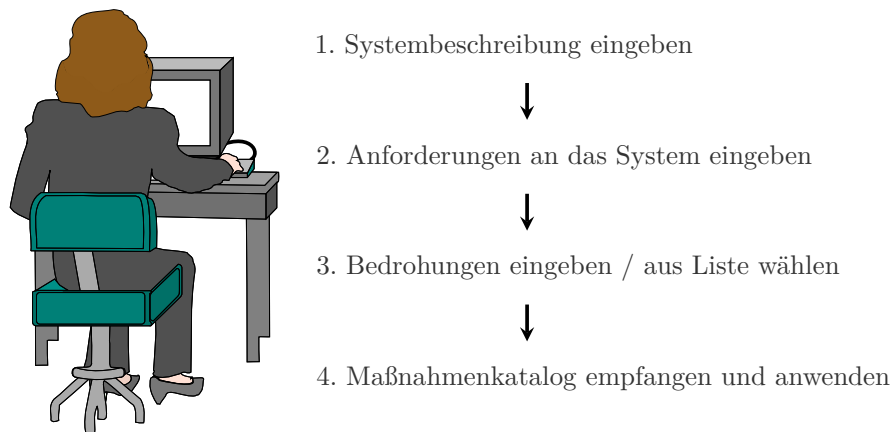


Abbildung 4.1.: Einfache Skizze des Programmablaufs

4.2. Hinweise zur Leistungsfähigkeit der Software

Generell ist davon auszugehen, dass nicht alle Aspekte, die im Bezug auf VoIP von Bedeutung sind, vom System beachtet werden. Menschliche Gefahren sind nur mühevoll bzw. gar nicht vorhersehbar. Aber auch andere Risiken können vermutlich vom System nicht korrekt eingestuft werden, da sie bei jeder Installation variieren. Im Folgenden sind die typischen Aspekte von VoIP-Sicherheit aufgeführt [Bad10, S. 448f]:

- technische Aspekte
 - Konfiguration und Installation von technischen Geräten und Software
 - Stromnetzanbindung
 - bauliche Trennung und Zugang von außen
 - Sicherheitsmechanismen (Zugriffsschutz, Firewall, ...)
 - Auditing und Monitoring
- organisatorische Aspekte
 - Passwort-Management
 - Benutzer- und Berechtigungsverwaltung
- menschliche Aspekte
 - Handhabungsfehler
 - kriminelle Handlungen
- geschäftliche Aspekte
 - Offenlegung von Kundendaten
 - vor Konkurrenz geschützte Verbindungen
- rechtliche Aspekte
 - private VoIP-Nutzung der Mitarbeit
 - Gebührenbetrug
 - Haftung und Beweissicherung im Streitfall

Nicht alle Kategorien kann ein Expertensystem abdecken. Allerdings sollte durch gezielte Fragen eine Möglichkeit für Ratschläge und Richtlinien geschaffen werden. Dabei ist zu beachten, dass zu viele für den Benutzer nicht relevante Empfehlungen ein Desinteresse auslösen könnten. In den nächsten Abschnitten wird erläutert, wie man diese Vorschläge sinnvoll einschränken kann.

4.3. Ansätze für Datenerhebung

Für den Ablauf der Datenerhebung gibt es verschiedene Ansätze. Einige haben eine höhere Benutzbarkeit, was vor allen technisch unerfahrenen Anwendern (Privatanwender) zugute käme. Andere Ansätze stellen einen hohen Anspruch an die Intelligenz des Systems. Wird diese nicht richtig implementiert, würden Anwender sich nicht auf die Daten verlassen können. Im Folgenden werden drei Ansätze beschrieben.

4.3.1. Maßnahmeneingrenzung durch Ausschlussprinzip

Eine erste Variante umfasst das Ausschlussprinzip. Der Benutzer wählt einen Bereich der Installation aus, an dem er nichts verändern kann oder will. Die Gründe dafür können weitreichend sein, wie zum Beispiel die baulichen Möglichkeiten oder Berechtigungen. Ein Privatanwender würde zum Beispiel nicht die Verkabelung neu verlegen oder eine alternative Stromversorgung installieren.

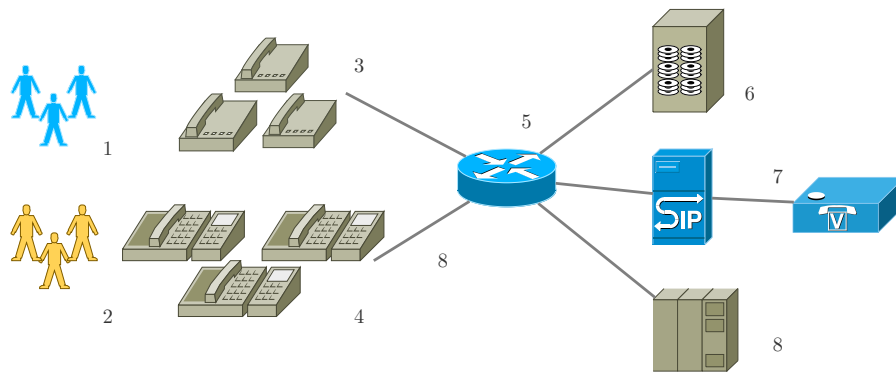


Abbildung 4.2.: Skizze einer Konfiguration

Im Programm könnte man dieses Verfahren mit einer Skizze der Installation ermöglichen. Der Nutzer klickt auf die Elemente, die er nicht verändern möchte. Dadurch werden die Elemente ausgegraut und später in den Empfehlungen nicht berücksichtigt. Auf der Abbildung 4.2 ist eine solche Skizze dargestellt. Die Tabelle 4.3.1 beinhaltet die Erklärungen für die Elemente des Modells.

Diese Möglichkeit würde für private Anwender mit wenig technischen Verständnis sinnvoll sein. Für größere Netzwerke darf natürlich nicht ein Bereich auf Grund von Zugangsproblemen ausgegrenzt werden. Deshalb wird diese Möglichkeit nicht weiter betrachtet.

4. Expertensystem

1	Benutzer ohne technischen Verständnis
2	Benutzer mit technischen Verständnis
3	Telefone ohne Authentifizierung oder persönliches Adressbuch
4	Telefone mit Authentifizierung und persönlichen Adressbuch
5	Backbone
6	Speicher für Adressbücher und Voicemail
7	Gateway
8	Andere Middleware
9	Infrastruktur

Tabelle 4.1.: Erklärung zu Abbildung 4.2

4.3.2. Systembeschreibungen vorschlagen lassen

Diese Variante befasst sich ausschließlich mit geplanten VoIP-Installationen. Für bereits aufgebaute Anlagen ist diese Methode nicht geeignet, da keine Informationen über schon installierte Elemente gesammelt werden.

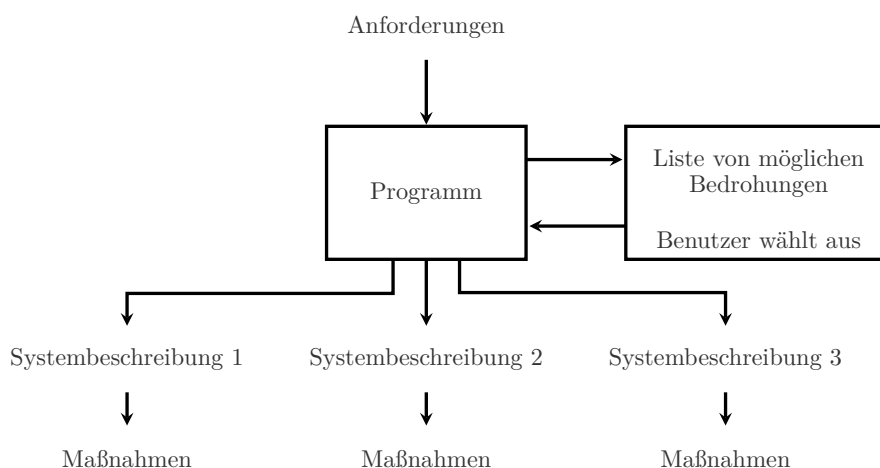


Abbildung 4.3.: Schematischer Ablauf des Programms nach Variante 4.3.2

Abbildung 4.3 zeigt einen schematischen Ablauf der Ein- und Aussagen. Zuerst stellt der Benutzer eine Liste von Anforderungen auf. Dieser resultierende Katalog sollte auf Vollständigkeit überprüft werden. Eine Änderung im Nachhinein wäre nur schwierig auf das System übertragbar. Die Benutzerschnittstelle übergibt die Zusammenstellung in einer geeigneten Form (zum Beispiel XML, siehe Abschnitt 4.4.2) an das System.

4. Expertensystem

Im nächsten Schritt zeigt das Programm eine vorselektierte Liste von Bedrohungen an. Zu jeder Gefährdung werden Erläuterungen und Eintrittswahrscheinlichkeiten signalisiert. Der Benutzer wählt nun die Elemente aus, die vom System berücksichtigt werden sollen.

Als Ausgabe werden nun mögliche Systemkonfigurationen gegeben. Parallel dazu könnten entsprechenden Maßnahmen zur Sicherung dieser Konfiguration angezeigt werden.

Die Berechnungen für die Vorschläge der Konfigurationen ist sehr komplex. Gute Resultate sind nur sehr aufwendig und mit einer guten Heuristik möglich. Auf Grund dieser Umstände wird diese Möglichkeit in dieser Arbeit nicht weiter ausgeführt.

4.3.3. Erweiterte Eingabe führt zu brauchbaren Ergebnissen

Eines der bedeutendsten Ansprüche an das System sind optimale Ergebnisse. Gibt das System nicht zutreffende Maßnahmen aus, wird es nicht benutzt. Um eine wertvolle Antwort des Programms zu erhalten, müssen die Eingaben sehr genau und spezifisch sein. Für einen guten Maßnahmenkatalog sind folgende Angaben wichtig:

- Systembeschreibung
- Anforderungen an die Installation
- Bedrohungen

Abbildung 4.4 zeigt ein Schema dieses Programmablaufs. Eine Erweiterungsmöglichkeit dieser Abfolge wäre die Einschränkung der Bedrohungen. Nachdem der Benutzer eine Systembeschreibung und die dazugehörigen Anforderungen angegeben hat, kann die Software nicht mögliche Gefahren aus der Liste streichen. Somit erhält der Anwender einen viel kürzeren Katalog von Gefährdungen und kann sich besser entscheiden.

Diese Methode ist von den Möglichkeiten her die erfolgversprechendste, falls das Programm die Eingaben richtig zuordnen kann. Deshalb ist es sehr wichtig, dass die Benutzerangaben für das Programm verständlich sind und in maschineller Form übergeben werden.

4. Expertensystem

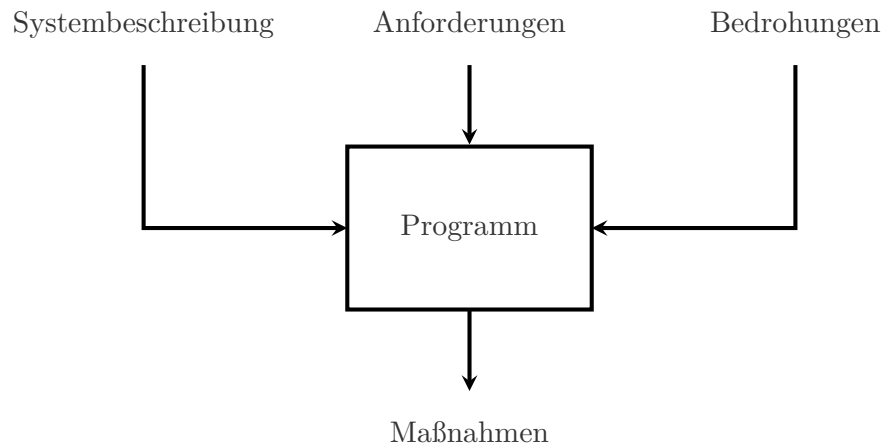


Abbildung 4.4.: Schema des Programmablaufs mit erweiterter Eingabe

4.4. Interaktion des Benutzers mit der Software

Die Qualität der resultierenden Maßnahmen und Empfehlungen des Programms sind direkt von den Eingaben des Benutzers abhängig. Eine Übermittlung in maschinell lesbarer Form ist deshalb unabdingbar. In den folgenden Abschnitten wird eine Möglichkeit zur Interaktion mit der Software dargestellt.

4.4.1. Benutzereingaben

Im weiteren Verlauf wird eine Trennung des Expertensystems in zwei Bereiche vorgenommen. Zum einen gibt es den Kern des Programms. Dort werden zum Beispiel die Entscheidungen für oder gegen das Anzeigen von Empfehlungen getroffen. Das andere Segment befasst sich mit der Dateneingabe. Es wird als GUI¹ bezeichnet. Abbildung 4.5 zeigt die Aufteilung und Interaktion der Software.

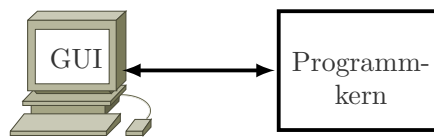


Abbildung 4.5.: GUI-Programmkern Interaktion

Die GUI ist nicht entscheidend für die erfolgreiche Dateneingabe. Wichtig ist nur, dass diese eine Übermittlung in eine maschinell lesbare Form vollbringt. Als Oberfläche könnte eine relativ einfache HTML-Seite dienen, die man mit einem üblichen

¹Graphical User Interface, zu Deutsch: grafische Benutzeroberfläche

4. Expertensystem

Browser aufrufen kann. Ein dort ausgefülltes Formular wird mittels HTTP-POST-Methode übermittelt und dann zu einer XML-Ausgabe (Abschnitt 4.4.2) umgewandelt. In Abbildung 4.6 ist eine Skizze dieser GUI dargestellt.

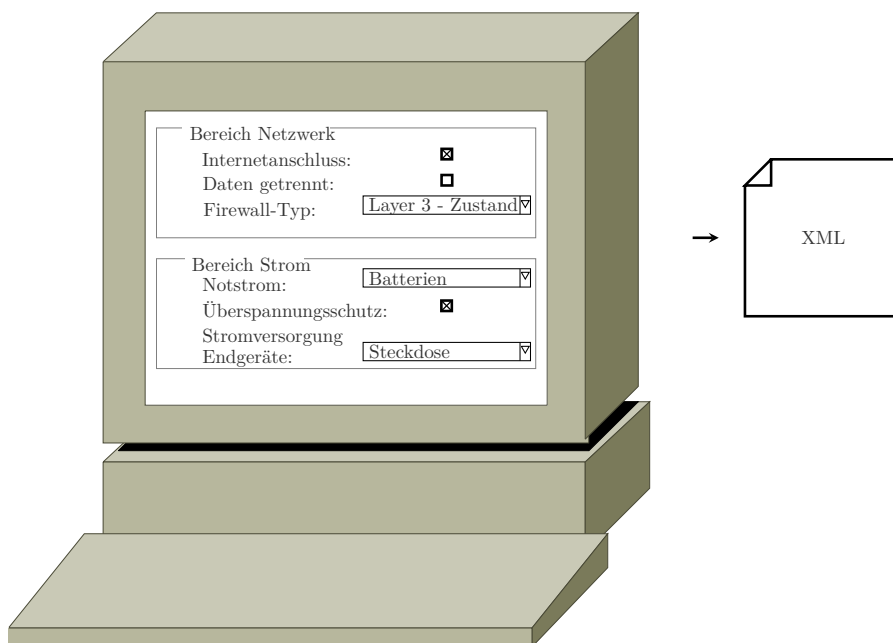


Abbildung 4.6.: Beispiel GUI

Diese GUI müsste natürlich Zusatzinformation enthalten, die für richtige Entscheidungen beim Ausfüllen sorgen. Diese Hinweise könnten dynamisch aus dem Internet nachgeladen werden, damit sie auf dem aktuellen Stand der Technik beruhen. Welche Auswahlfelder dem Benutzer zur Verfügung stehen, wird der GUI vom Programm mitgeteilt. Für diese Übermittlung wäre das gleiche Datenformat XML möglich.

4.4.2. Ein- und Ausgaben des Kerns durch XML

Generell ist davon auszugehen, dass jegliche Spezifikation nicht vollständig sein kann. Es sollte also eine Sprache gewählt werden, die dynamisch erweiterbar ist. Ein nachträglich eingefügter Schlüssel oder eine geänderte Anordnung sollte nicht die gesamte Kommunikation stören. Deswegen wird innerhalb dieser Arbeit auf XML² für die Beschreibungen gesetzt.

XML (Extensible Markup Language) dient zur Darstellung von hierarchisch angeordneten Strukturen in Form von Textdaten. Die Struktur wird in speziellen standardisierten Formaten definiert und kann somit gut ausgetauscht, geändert und erwei-

²Ausführungen zu XML: <http://www.w3.org/XML/>

4. Expertensystem

tert werden. Als Schemasprache wird in dieser Arbeit DTD³ verwendet. Sie reicht für die Zielsetzung dieser Arbeit aus und ist für das menschliche Auge schneller⁴ erfassbar.

Im Anhang A.1 sieht man eine beispielhafte DTD für ein Expertensystem, welches in Abschnitt 4.3.3 beschrieben wurde. Alle Elemente die für den Datenaustausch benötigt werden, sind dort definiert. Im weiteren Verlauf dieser Arbeit werden alle XML-Dateien auf diese Dokumenttypdefinition zurückgreifen.

4.4.3. Beispiel einer Eingabe

Im Folgenden wird eine beispielhafte Eingabe aller Daten für das Programm simuliert. Dabei konzentrieren sich die Fragen nur auf den physikalischen Bereich der VoIP-Installation. Auf Vollständigkeit wird dabei keinen Wert gelegt. Es soll viel mehr das Prinzip des Vorgangs gezeigt werden.

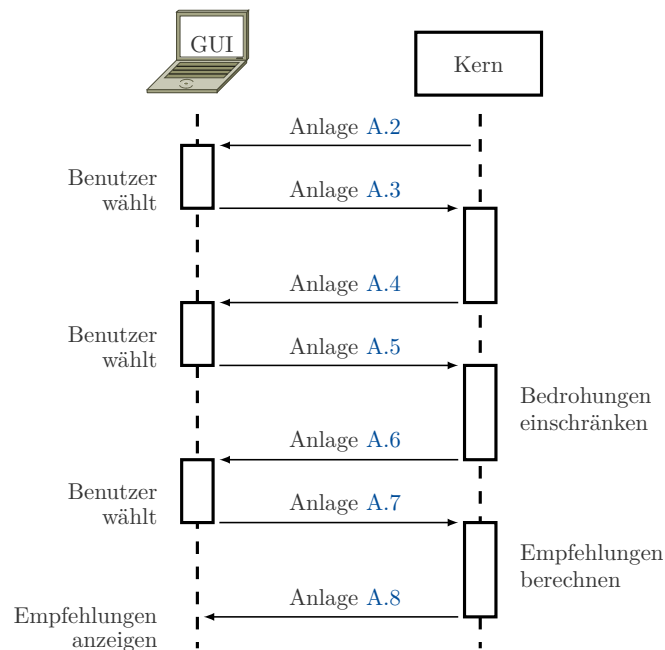


Abbildung 4.7.: Sequenzdiagramm mit XML-Nachrichten

Zuerst werden, wie die Abbildung 4.7 zeigt, die Daten für die Systembeschreibung benötigt. Dafür schickt das Programm Fragen an die GUI. In der Tabelle 4.4.3 sind diese Fragen aufgeführt. Die zweite Spalte bezeichnet dabei den von der GUI zurückzugebenden Wert.

³Dokumenttypdefinition, definiert in ISO/IEC 19757 Part 9

⁴Im Vergleich zu XML Schema (XSD), <http://www.w3.org/TR/xmlschema-0/>

4. Expertensystem

Frage	bool oder enum
Ist ihr Serverraum abschließbar/verriegelt?	bool
Ist eine Authentifikation für den Zugriff erforderlich?	bool
Wie wird die Authentifikation durchgeführt?	Smartcard Einmal-Passwörter
Ist der Zugang oder Serverraum videoüberwacht?	bool
Wie sind die Kabeltrassen verlegt?	Unterputz Kabelkanal Freiliegend
Gibt es eine Variation einer USV?	bool
Werden die Endgeräte über Power-over-Ethernet versorgt?	bool
Ist eine Trennung von Sprach- und Datennetz vorhanden?	bool

Tabelle 4.2.: Fragen für den physikalische Bestand

Diese Fragen bauen teilweise aufeinander auf. Im Anhang [A.2](#) befindet sich dieser Katalog als XML-Datei, wobei auch ersichtlich wird, dass einige Fragen nur bei bestimmten Antworten gestellt werden. Außerdem wird im Anhang [A.3](#) eine mögliche Antwort der Benutzerschnittstelle gegeben. Diese enthält die fiktiven Eingaben des Benutzers und somit die Antworten auf die Fragen.

Nun werden Informationen zu den Anforderungen der Installation benötigt. Auch hierfür generiert das Programm Fragen und sendet sie als XML-Datei (Anhang [A.4](#)) an die GUI. Tabelle [4.4.3](#) zeigt diese Fragen übersichtlich.

Frage	bool oder enum
Wo wird Ihr System eingesetzt?	Privat Unternehmen Behörde
Wie viele Personen werden das System benutzen?	int
Wie wichtig ist Ihnen die Verfügbarkeit des Systems?	int 1-5
Wie wichtig ist Ihnen die Integrität des Systems?	int 1-5
Ist mit Identitätsbetrug (Gebührenbetrug) zu rechnen?	bool
Wie wichtig ist Ihnen die Vertraulichkeit des Systems?	int 1-5

Tabelle 4.3.: Fragen zu den Anforderungen an das System

4. Expertensystem

Der Benutzer wählt die passenden Antworten für sein System aus und die graphische Oberfläche übergibt die Angaben als XML-Datei (Anhang A.5) an den Kern. Dabei hält sich der XML-Aufbau an die gegebene DTD (Anhang A.1).

Der Systemkern berechnet nun welche Bedrohungen laut Systembeschreibung nicht mehr zutreffen können. Im aktuellen Fall gibt es keine Risiken im Bereich der Serverräume, da diese ausreichend gesichert sind. Für die restlichen Gefahren wird eine Liste per XML (Anlage A.6) an die GUI geschickt. Der Benutzer antwortet beispielsweise auf beide Fragen mit *Ja*. Dies wird im Anhang A.7 dargestellt.

4.4.4. Beispiel der Ausgabe von Empfehlungen und Vorschlägen

Im vorherigen Abschnitt 4.4.3 wurde eine beispielhafte Eingabe dargestellt. Nachdem das System nun alle nötigen Informationen gesammelt hat, wird ein Empfehlungs- und Vorschlagkatalog erstellt. Dieser wird mittels XML (Anlage A.8), welche sich an die DTD (Anlage A.1) hält, an die GUI gesandt. Eine graphische Ausgabe könnte wie folgt aussehen:

- Physikalischer Schutz
 - Sicherungsmaßnahmen der Räume gegen Stromausfall, Wasserschaden und Feuer erhöhen.
 - Kabeltrassen durch Verkleidung oder Unterputzverlegung schützen.
- Stromversorgung
 - Unterbrechungsfreie Stromversorgung (USV)
 - * Middleware wird korrekt heruntergefahren
 - * Benachrichtigung durch SMS/E-Mail/Pieper
 - Falls USV eingebaut wird, kann auch Power-over-Ethernet (PoE) verwendet werden.
- Trennung von Sprach- und Datennetz
 - Physikalische Trennung
 - Logische Trennung

Diese Darstellung ist relativ simpel und dient nur der Veranschaulichung der XML-Daten. Zusätzlich zu jedem Stichpunkt könnte das Programm einen Link einblenden, der den Benutzer zu mehr Informationen führt.

5. Zusammenfassung

In der Arbeit wurde gezeigt, dass es eine automatisierte Checkliste für sichere VoIP-Installationen geben kann. Im Folgenden wird ein kurzer Ausblick über die weitere Arbeit in diesem Thema gegeben. In dem abschließenden Fazit werden die Resultate der Arbeit festgestellt.

5.1. *Ausblick*

Diese Arbeit bietet einen Überblick über die aktuelle Bedrohungslage im Bereich der VoIP-Installationen. Damit dieser Katalog auch weiterhin der Situation entspricht und mit moderneren Systemen mithalten kann, muss ein digitales Format für die Gefährdungen und dazugehörigen Maßnahmen gefunden werden. Diese sind dann regelmäßig um neuere Regeln zu erweitern.

Das beschriebene Programm könnte mit Hilfe von bereits existierenden Bibliotheken für Expertensysteme implementiert werden. Dabei ist allerdings besonders auf eine gute Wartungsfähigkeit der Kataloge zu achten. Eine automatische Suche nach neuen Zusammenstellungen über das Internet ist eine Voraussetzung für ein praktikables Programm.

Nach der Implementierung müssten die Fragen für die Administratoren aufgestellt werden. Diese sind besonders wichtig, denn nur durch sie wird das Programm brauchbar. Gegebenfalls sollten Sprachwissenschaftler diese Aufgabe übernehmen.

5.2. *Fazit*

Ziel dieser Arbeit war es, zu überprüfen ob eine automatisierende Hilfestellung für die sichere Installation von VoIP-Telefonanlagen möglich ist und diese gegebenenfalls darzustellen.

Die Ausarbeitung der Bedrohungslage liefert einen Einblick in die benötigten Informationen für ein Expertensystem. Dabei wird auf einige kritische Bereiche der Installation ein besonderes Augenmerk gelegt.

5. Zusammenfassung

Die Sicherungsmaßnahmen leiten sich direkt aus den Gefährdungen ab. Jeder einzelne Vorschlag wurde mit Kennzeichen versehen, um einem Programm differenzierte Anzeigemöglichkeiten zu geben. Diese Markierungen der Ratschläge können nicht wissenschaftlich belegt werden, sondern spiegeln ein Aufwand/Nutzen-Verhältnis wider. Für alle in Kapitel 2 aufgelisteten Bedrohungen sind Beseitigungshinweise oder Präventivmaßnahmen aufgezeigt worden.

Mit Hilfe der gewonnenen Informationen wurden im Kapitel 4 die Möglichkeit eines Expertensystems diskutiert. Aus den vorgeschlagenen Varianten der Datenerhebung konnte eine näher erläutert werden. Ein möglicher Ablauf des Programms wurde anhand eines Beispiels dargestellt. Im Anhang sind die dazugehörigen XML-Nachrichten enthalten.

Ein Expertensystem für die sichere Installation von VoIP-Telefonanlagen ist in einem gegebenen Rahmen möglich. Die Qualität der Ratschläge wird aber immer von den Eingaben des Benutzers und des gegebenen Katalogs abhängen.

A. Quellcode

Listing A.1: DTD für die XML-Dokumente

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!ELEMENT answers (answer)*>
3 <!ELEMENT answer (name,value)>
4 <!ELEMENT name (#PCDATA)>
5 <!ELEMENT value (#PCDATA)>
6 <!ELEMENT questions (question)*>
7 <!ELEMENT question (return,text,type,onTrue?,onFalse?)>
8 <!ELEMENT return (#PCDATA)>
9 <!ELEMENT text (#PCDATA)>
10 <!ELEMENT type (bool|int|enum|range)>
11 <!ELEMENT bool EMPTY>
12 <!ELEMENT int EMPTY>
13 <!ELEMENT range (#PCDATA)>
14 <!ELEMENT enum (elem)+>
15 <!ELEMENT elem (#PCDATA)>
16 <!ELEMENT onTrue (question)*>
17 <!ELEMENT onFalse (question)*>
18 <!ELEMENT advices (advice|adviceGroup)+>
19 <!ELEMENT adviceGroup (name,advices)>
20 <!ELEMENT advice (#PCDATA)>
```

Listing A.2: Fragen zu Layer 1

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE questions SYSTEM "example.dtd">
3 <questions>
4   <question>
5     <return>serverRoom</return>
6     <text>Ist ihr Serverraum abschließbar/verriegelt?</text>
7     <type>
8       <bool />
9     </type>
10    <onTrue>
11      <question>
12        <return>serverRoomAuthentication</return>
13        <text>Ist eine Authentifikation für den Zugriff erforderlich?</text>
14        <type>
15          <bool />
16        </type>
17        <onTrue>
18          <question>
19            <return>serverRoomAuthenticationType</return>
20            <text>Wie wird die Authentifikation durchgeführt?</text>
21            <type>
22              <enum>
23                <elem>Smartcard</elem>
24                <elem>Einmal-Passwörter</elem>
25              </enum>
26            </type>
27          </question>
28        </onTrue>
29      </question>
30    </onTrue>
31  </question>
32 <question>
33   <return>serverRoomVideo</return>
34   <text>Ist der Zugang oder Serverraum Videoüberwacht?</text>
35   <type>
```

A. Quellcode

```
36     <bool />
37   </type>
38 </question>
39 <question>
40   <return>cableRoute</return>
41   <text>Wie sind die Kabeltrassen verlegt?</text>
42   <type>
43     <enum>
44       <elem>Unterputz</elem>
45       <elem>Kabelkanal</elem>
46       <elem>Freiliegend</elem>
47     </enum>
48   </type>
49 </question>
50 <question>
51   <return>usv</return>
52   <text>Gibt es eine Variation einer USV?</text>
53   <type>
54     <bool />
55   </type>
56   <onTrue>
57     <question>
58       <return>usvPoe</return>
59       <text>Werden die Endgeräte über Power-over-Ethernet versorgt?</text>
60       <type><bool/></type>
61     </question>
62   </onTrue>
63 </question>
64 <question>
65   <return>separationVoiceData</return>
66   <text>Ist eine Trennung von Sprach- und Datennetz vorhanden?</text>
67   <type>
68     <bool />
69   </type>
70 </question>
71 </questions>
```

Listing A.3: Antworten zu Layer 1

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE answers SYSTEM "example.dtd">
3 <answers>
4   <answer>
5     <name>serverRoom</name>
6     <value>true</value>
7   </answer>
8   <answer>
9     <name>serverRoomAuthentication</name>
10    <value>true</value>
11  </answer>
12  <answer>
13    <name>serverRoomAuthenticationType</name>
14    <value>Smardcard</value>
15  </answer>
16  <answer>
17    <name>serverRoomVideo</name>
18    <value>>false</value>
19  </answer>
20  <answer>
21    <name>cableRoute</name>
22    <value>Kabelkanal</value>
23  </answer>
24  <answer>
25    <name>usv</name>
26    <value>>false</value>
27  </answer>
28  <answer>
29    <name>separationVoiceData</name>
30    <value>true</value>
31  </answer>
32 </answers>
```

A. Quellcode

Listing A.4: Fragen zu Anforderungen

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE questions SYSTEM "example.dtd">
3 <questions>
4   <question>
5     <return>systemLocation</return>
6     <text>Wo wird Ihr System eingesetzt?</text>
7     <type>
8       <enum>
9         <elem>Privat</elem>
10        <elem>Unternehmen</elem>
11        <elem>Behörde</elem>
12      </enum>
13    </type>
14  </question>
15  <question>
16    <return>usingPersons</return>
17    <text>Wie viele Personen werden das System benutzen?</text>
18    <type>
19      <int />
20    </type>
21  </question>
22  <question>
23    <return>systemAvailability</return>
24    <text>Wie wichtig ist Ihnen die Verfügbarkeit des Systems?</text>
25    <type>
26      <range>1-5</range>
27    </type>
28  </question>
29  <question>
30    <return>systemIntegrity</return>
31    <text>Wie wichtig ist Ihnen die Integrität des Systems?</text>
32    <type>
33      <range>1-5</range>
34    </type>
35  </question>
36  <question>
37    <return>systemIdentityTheft</return>
38    <text>Ist mit Identitätsbetrug (Gebührenbetrug) zu rechnen?</text>
39    <type>
40      <bool />
41    </type>
42  </question>
43  <question>
44    <return>systemConfidentiality</return>
45    <text>Wie wichtig ist Ihnen die Vertraulichkeit des Systems?</text>
46    <type>
47      <range>1-5</range>
48    </type>
49  </question>
50 </questions>
```

A. Quellcode

Listing A.5: Antworten zu Anforderungen

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE answers SYSTEM "example.dtd">
3 <answers>
4   <answer>
5     <name>systemLocation</name>
6     <value>Unternehmen</value>
7   </answer>
8   <answer>
9     <name>usingPersons</name>
10    <value>150</value>
11  </answer>
12  <answer>
13    <name>systemAvailability</name>
14    <value>4</value>
15  </answer>
16  <answer>
17    <name>systemIntegrity</name>
18    <value>3</value>
19  </answer>
20  <answer>
21    <name>systemIdentityTheft</name>
22    <value>5</value>
23  </answer>
24  <answer>
25    <name>systemConfidentiality</name>
26    <value>3</value>
27  </answer>
28 </answers>
```

Listing A.6: Fragen zu Bedrohungen

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE questions SYSTEM "example.dtd">
3 <questions>
4   <question>
5     <return>riskCableRoute</return>
6     <text>Soll die Gefahr an Kabeltrassen, Kabelverteilersysteme, Datenverteiler beachtet werden?</text>
7     <type>
8       <bool />
9     </type>
10  </question>
11  <question>
12    <return>riskPower</return>
13    <text>Sollen stromtechnische Bedrohungen berücksichtigt werden?</text>
14    <type>
15      <bool />
16    </type>
17  </question>
18 </questions>
```

Listing A.7: Antworten zu Bedrohungen

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE answers SYSTEM "example.dtd">
3 <answers>
4   <answer>
5     <name>riskCableRoute</name>
6     <value>true</value>
7   </answer>
8   <answer>
9     <name>riskPower</name>
10    <value>true</value>
11  </answer>
12 </answers>
```

A. Quellcode

Listing A.8: Empfehlungen und Vorschläge

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE advices SYSTEM "example.dtd">
3 <advices>
4   <adviceGroup>
5     <name>Physikalischer Schutz</name>
6     <advices>
7       <advice>Sicherungsmaßnahmen der Räume gegen Stromausfall, Wasserschaden und Feuer erhöhen.</advice>
8     </advices>
9   </adviceGroup>
10  <adviceGroup>
11    <name>Stromversorgung</name>
12    <advices>
13      <adviceGroup>
14        <name>Unterbrechungsfreie Stromversorgung (USV)</name>
15        <advices>
16          <advice>Middleware wird korrekt heruntergefahren</advice>
17          <advice>Benachrichtigung durch SMS/E-Mail/Pieper</advice>
18        </advices>
19      </adviceGroup>
20      <advice>Falls USV eingebaut wird, kann auch Power-over-Ethernet (PoE) verwendet werden.</advice>
21    </advices>
22  </adviceGroup>
23  <adviceGroup>
24    <name>Trennung von Sprach- und Datennetz</name>
25    <advices>
26      <advice>Physikalische Trennung</advice>
27      <advice>Logische Trennung</advice>
28    </advices>
29  </adviceGroup>
30 </advices>
```

Abbildungsverzeichnis

1.1. Ein- und Ausgaben des Systems	3
2.1. Skizze eines gehärteten Betriebssystems mit entfernten Komponenten	17
2.2. Endgeräte im Netzwerk	20
2.3. Angriff über WLAN ist meist viel einfacher	22
3.1. Beispiel für die Absetzung eines Notrufs	31
4.1. Einfache Skizze des Programmablaufs	38
4.2. Skizze einer Konfiguration	40
4.3. Schematischer Ablauf des Programms nach Variante 4.3.2	41
4.4. Schema des Programmablaufs mit erweiterter Eingabe	43
4.5. GUI-Programmkern Interaktion	43
4.6. Beispiel GUI	44
4.7. Sequenzdiagramm mit XML-Nachrichten	45

Tabellenverzeichnis

2.1. Bedrohungen physikalische Ebene	7
2.2. Bedrohungen Sicherungsschicht	9
2.3. Bedrohungen Vermittlungsschicht	11
2.4. Bedrohungen Transportschicht	13
2.5. Übersicht der Netzwerkattacken	14
3.1. Abkürzungen der Schutzbedürfnisse	24
4.1. Erklärung zu Abbildung 4.2	41
4.2. Fragen für den physikalische Bestand	46
4.3. Fragen zu den Anforderungen an das System	46

Literaturverzeichnis

- [AB07] ANATOL BADACH, Erwin H.: *Technik der IP-Netze*. Hanser, 2007. – ISBN 978-3-446-21935-9
- [Bad10] BADACH, Anatol: *Voice over IP - Die Technik*. Hanser, 2010. – ISBN 987-3-446-41772-4
- [BSI05] BSI: Studie zur Sicherheit von VoIP / BSI. 2005. – Forschungsbericht. – ISBN 3-89817-539-1
- [BSI09] BSI: *IT-Grundschutzhandbuch*. URL: <http://www.bsi.bund.de/gshb/deutsch/>, 2009
- [Fis08] FISCHER, Dr. J.: *VoIP Praxisleitfaden*. Hanser, 2008. – ISBN 978-3-446-41188-3
- [JD00] JONATHAN DAVIDSON, James P.: *Voice Over IP - Grundlagen*. Cisco Press, 2000. – ISBN 3-8272-5800-6
- [Sie09] SIEGMUND, Prof. Dr.-Ing. G.: *Technik der Netze - Band 2*. 6. VDE, 2009. – ISBN 978-3-7785-4063-3
- [Sie10] SIEGMUND, Prof. Dr.-Ing. G.: *Technik der Netze - Band 1*. 6. VDE, 2010. – ISBN 978-3-8007-3219-7

Selbstständigkeitserklärung

Ich versichere, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Rostock, den **01. April 2011**