FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Unterstützung der IT–Sicherheit von VoIP–Infrastrukturen durch die Verwendung spezialisierter VoIP–Firewalls

Bakkalaureatsarbeit

zur Erlangung des akademischen Grades

Bakk.tech.

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Philipp Schaden
Matrikelnummer 0626698

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung: Thomas Grechenig
Mitwirkung: Florian Fankhauser

Wien, 11.11.2011

(Unterschrift Verfasser/In)

(Unterschrift Betreuung)

Unterstützung der IT–Sicherheit von VoIP–Infrastrukturen durch die Verwendung spezialisierter VoIP–Firewalls

Bakkalaureatsarbeit

zur Erlangung des akademischen Grades

Bakk.tech.

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Philipp Schaden
Matrikelnummer 0626698

ausgeführt am
Institut für Rechnergestützte Automation
Forschungsgruppe Industrial Software
der Fakultät für Informatik der Technischen Universität Wien

Betreuung: Thomas Grechenig
Mitwirkung: Florian Fankhauser

Wien, 11.11.2011

Liste der noch zu erledigenden Punkte

Eidesstattliche Erklärung

Philipp Schaden
Aschau 93, 7432 Oberschützen

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

I hereby declare that I am the sole author of this thesis, that I have completely indicated all sources and help used, and that all parts of this work - including tables, maps and figures - if taken from other works or from the internet, whether copied literally or by sense, have been labelled including a citation of the source.

(Ort, Datum) (Unterschrift Verfasser/In)

Danksagung

Bedanke möchte ich mich hiermit bei allen Personen, die mir geholfen haben, diese Arbeit fertigzustellen.

Abstract

According to the guidelines of the faculty, an abstract in English has to be inserted here.

Keywords

Keyword, important, SubjectOfMyPaper, FieldOfWork.

Kurzfassung

Hier fügen Sie die Kurzfassung auf Deutsch gemäß den Vorgaben der Fakultät ein.

Schlüsselwörter

Schlüsselwörter, wichtig, ThemaMeinerArbeit, Arbeitsgebiet.

Inhaltsverzeichnis

1 Einleitung

1.1 Problemstellung

1.1.1 Allgemeine Problemstellung

Voice Over Internet Protocol (kurz VoIP) ist eine sehr stark wachsende und häufig verwendete Technologie. Insbesondere in großen – aber auch mittelgroßen - Unternehmen findet diese Kommunikationsart Anklang. Durch diesen hohen Verbreitungsgrad sind viele Sicherheitsprobleme entstanden. Einige solcher Probleme werden im Zuge dieser Arbeit näher beschrieben.
In dieser wissenschaftlichen Arbeit werden daher die Sicherheit in VoIP-Netzwerken erörtert und die Absicherungsmöglichkeiten mittels einer speziellen VoIP-Firewall ergründet bzw. Sicherheitslücken und Sicherheitsrisiken aufgezeigt.

1.1.2 Detaillierte Problemstellung

Im Rahmen dieser wissenschaftlichen Arbeit werden die Sicherheitsaspekte einer Voice Over IP Infrastruktur näher erörtert und die dabei entstehende Problematik der Absicherung diskutiert. In den letzten Jahren wurden VoIP-Netzwerke immer interessantere Ziele für Angriffe aus dem Netz. Die Absicherung dieser Netzwerke ist daher ein sehr kritischer Bereich und eine ebenso herausfordernde Aufgabe.
Für Unternehmen ist ein gesichertes Netzwerk die Basis eines zuverlässigen Betriebs und soll daher möglichst ausfallsicher sein. Im Themenbereich Sicherheit im Netzwerk gibt es eine Reihe von Hypothesen zu deren Absicherung. Im Rahmen dieser Arbeit wird eine Testumgebung in einem Labor eingerichtet, welche VoIP-Komponenten enthält. In Testläufen werden Angriffe simuliert, auf einer speziellen VoIP-Firewall getestet und die Auswirkungen auf die VoIP-Umgebung ermittelt. Die Ergebnisse werden anschließend analysiert.

Nicht nur konventionell vernetzte Systeme sind Ziele von Attacken, sondern auch VoIP- Netzwerke, welche die Schwachstellen von diesen konventionellen IP-basierten Netzwerken erben. So sind beispielsweise Man-in-the-Middle oder Denial of Service (kurz DoS) Attacken große Gefahrenquellen, die einen störungsfreien Betrieb oftmals verhindern können. Darüber hinaus gibt es auch Angriffsmethoden, die speziell auf VoIP abzielen und von Hung et al. beschrieben werden. [15]

1.2 Erwartetes Resultat

Fachliches Ziel dieser Arbeit ist die Darstellung von relevanten Problemen im Bereich von VoIP sowohl im unternehmerischen Umfeld als auch im privaten Bereich. Darauf aufbauend sollen Lösungsmuster dargestellt und analysiert werden.

Es sollen bestehende und „vererbte“ Probleme demonstriert und mit Lösungsmöglichkeiten bzw. Abhilfen versehen werden. Danach sollen die recherchierten Problemlösungen anhand einer Testumgebung im Labor mittels einer speziellen VoIP-Firewall getestet und dokumentiert werden.

Konkret wird auf die Fragestellung eingegangen, wie sich eine IT-Landschaft mit VoIP-Einsatz gegen gegenwärtige Probleme (wie z.B. DoS (Denial of Service), Phishing, Spoofing) absichern kann und welche Effekte dabei auftreten können. Ein reibungsloser Betrieb der IT-Umgebung soll soweit wie möglich aufrechterhalten werden. Wie Qu et al. in [18] beschreiben, gibt es im Bereich der Absicherung von kleinen bis großen Firmennetzwerken etablierte und gereifte Mechanismen und Konzepte, die vom Großteil der Firmen verwendet werden.
Der Einsatz von möglichst vielen Mechanismen und Geräten bedeutet nicht, dass der Schutzfaktor maximal ist. Somit ist es aus vielerlei Standpunkt wichtig, entsprechende Methoden und Vorgehensweisen bei der Absicherung von VoIP zu evaluieren und zu vergleichen. Am Beginn der Arbeit werden zuerst grundlegende Themen zu IT-Sicherheit, VoIP und Firewalls beschrieben und abgehandelt. Darauf aufbauend bildet das Kapitel zu Angriffe auf VoIP einen detaillierten Einblick in die Gefahrenwelt einer VoIP-Umgebung. Es wird beschrieben, wie Angriffe entstehen können und woher diese überhaupt kommen können. Anschließend werden Absicherungsmechanismen vorgestellt und deren Wirksamkeit beim Einsatz gegen verschiedene Angriffsszenarien deutlich gemacht.

In den letzten beiden Abschnitten der Arbeit wird der praktische Teil hervorgehoben. Hierbei werden detaillierte Angriffsschritte vorgenommen und protokolliert sowie Versuche zur Abwehr und Einsatzmöglichkeit und Konfigurationsmethoden von speziellen Firewalls näher erläutert und verglichen. Dabei wird auf die Einsetzbarkeit, Sinnhaftigkeit und Effizienz genauer eingegangen.

Am Schluss folgt eine Zusammenfassung der Arbeit sowie ein Ausblick auf kommende Themen.

1.3 Methodisches Vorgehen

Basierend auf großteils theoretischer Ausarbeitung und aktueller Literatur wird die Sicherheit von VoIP-Netzwerken mittels spezialisierter Firewalls im Zuge dieser Ausarbeitung dargestellt. Ziel der Arbeit ist eine detaillierte Darstellung von Angriffsszenarien auf VoIP und wie man möglichen Angriffen entgegenwirken kann. Als Werkzeug soll diesbezüglich eine VoIP-Firewall verwendet werden.
Hinzu kommt ein praktischer Teil, welcher in die Arbeit einfließen wird. Hierbei wird eine spezielle Firewall für VoIP-Netzwerke herangezogen, um Angriffe und Methoden zur Abwehr testen und beobachten zu können. Zusätzlich werden die Ergebnisse empirischer und praktischer Art gesondert und sorgfältig dokumentiert.
Das methodische Vorgehen bei der Verfassung dieser Arbeit basiert auf dem Einlesen in die entsprechende Fachliteratur, welche in der ersten Phase zur Bearbeitung der Basisthemen Security, Voice over IP und Firewall-Absicherung dient und in der darauffolgenden Phase Fachwissen zum Thema VoIP-Firewalls in verschiedenen VoIP-Infrastrukturen liefert.
Das Ergebnis dieser Fachrecherche ist eine Aufarbeitung des Themas VoIP-Security und die aktuellsten technischen Möglichkeiten zum Einsatz von Firewalls in diesem Bereich. Aufbauend auf dem Wissen aus Grundlagen und Fachliteratur kann ein Vergleich bzw. eine Bewertung und Auswahl der Methoden und Empfehlungen vorgenommen werden.

1.4 State of the Art

Ronniger et al. stellen in [19] fest, dass viele Attacken auf VoIP-Netzwerke bekannt sind - aber es dennoch keine vollkommen abgesichert VoIP-Infrastruktur gibt. VoIP-Netzwerke sind immer noch gegen verschiedenartige Attacken anfällig.
Um laut Cao et al. in [8] diese testen zu können, müssen bestimmte Richtlinien für Testumgebungen eingehalten werden.
In diesen Testumgebungen werden spezielle Werkzeuge und Methoden bereitgestellt, welche von Abdelnur et al. in [1] beschrieben werden.
Strobel schreibt in [9], dass der zentrale Punkt einer für diese Arbeit relevanten Testumgebung die VoIP-Firewall bildet. Diese ist laut Coulibaly et al. in [9] speziell ausgerichtet und der zentrale Angriffspunkt des Testnetzwerkes.
Aber laut Butcher et al. in [7] muss auch VoIP-Software auf Schwachstellen getestet werden.
Eckert schreibt in [10] wie wichtig es ist, dass die vordefinierten Sicherheitsziele - wie z.B. jene des Bundesamtes für Sicherheit in der Informationstechnologie (kurz BSI) - eingehalten werden und sich Mechanismen einbetten lassen, die gegen Angriffe wirksam sind.
Drei Muster spezifischer Sicherheitsprobleme auf VoIP-Implementierungen bezogen treten häufig auf: (A) sicherer Verkehr durch eine Firewall bzw. eines NATs; (B) Entdeckung und Abschwächung von DDoS (Distributed-Denial-of-Service) Attacken; und (C) Absicherung gegen das heimliche Abhören. Da Verkäufer viele Produkte mit ähnlicher oder überschneidender Funktionalität entwerfen, ist es wichtig, dass man sich vor der Anschaffung ein Design für die Absicherung des Zielnetzwerkes überlegt hat - Anwar et al. beschreiben einen Designvorschlag zur Absicherung in [2] .
Falls ein Netzwerk wenige Sicherheitsvorkehrungen aufweist, ist es laut Endler et al. [12] unschwer möglich, VoIP-Telefone bzw. das gesamte VoIP-Netzwerk zu hacken.
Egger et al., Eren et al. und Porter beschreiben in [11] ,[13] ,[17] Möglichkeiten, um die richtigen Sicherheitsmaßnahmen für eine gegebene Infrastruktur zu wählen. Weiters soll man sich Vorkenntnisse durch Recherche aneignen und in andere Erfahrungsberichte einlesen.

2 Grundlagen der IT-Sicherheit

In diesem Kapitel werden allgemeine Begriffe wie zum Beispiel die Grundbegriffe der Sicherheit, diverse Sicherheitsziele aus dem Grundschutzkatalog sowie Schutzbedarf Bedrohungsanalysen behandelt.
Weiters wird eine klare Grenze zwischen Sicherheit und IT-Sicherheit gezogen. Abschließend wird auf das Teilgebiet der VoIP-Sicherheit eingegangen.

2.1 Sicherheitsziele

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt folgende Sicherheitsziele (security objectives) in einem Sicherheitskatalog: [6]

- Verfügbarkeit (availability)
- Integrität (integrity)
- Vertraulichkeit (privacy, confidentialty)

2.1.1 Verfügbarkeit

Verfügbarkeit (availability) meint die Eigenschaft eines Systems, innerhalb eines bestimmten Zeitraums mit einer bestimmten Wahrscheinlichkeit die vom eingesetzten System erwarteten Anforderungen zu erfüllen. Die Verfügbarkeit zählt zu den Qualitätsmerkmalen einer IT-Landschaft.

2.1.2 Integrität

Unter der Integrität (integrity) von Informationen versteht man die Vollständigkeit und Korrektheit (Unversehrtheit) der übertragenen Daten auf Sender- und auch Empfängerseite. Dabei wird davon ausgegangen, dass keine Manipulation der Daten auf dem Transportweg durchgeführt wurden und somit unveränderte Daten verschickt wurden. Um diese Datenintegrität an beiden Kommunikationsenden zu kontrollieren, kann man verschiedene Kontrollmethoden verwenden: Zum Beispiel (Z.B.) Hash-Verfahren, message authentification codes oder digitale Signaturen. Um diesen Mechanismus durchführen zu können, sind die Inhalte der Daten mit den Kontrollmethoden direkt verknüpft. Durch unzureichende Integritätsprüfung können fehlerhafte Datensätze entstehen: Z.B. Fehlerhafte Produktionen, Falsche Warenlieferungen oder Verbuchungsfehler. In den letzten Jahren wird dem Verlust an Authentizität als Teil der Datenintegrität verstärktes Augenmerk gewidment. Im schlimmsten Fall wirken sich Fehler auf Zahlungen und Identitäten aus, welche an nicht berechtigte Personen ausgestellt werden. So kann es beispielsweise zu Identitätsdiebstahl kommen. [4] [16] [3]

2.1.3 Vertraulichkeit

Um eine sichere und effektive Datenübertragung und Verarbeitung zu gewährleisten, muss eine hohe Vertraulichkeit (confidentiality) erreicht werden und erhalten bleiben. Allgemein lässt sich die Vertraulichkeit als Gewährleistung beschreiben, bei welcher die zu verarbeitenden Daten nur an jene Personen zugestellt und verfügbar gemacht werden, die auch die nötigen Berechtigungen besitzen. Auf der anderen Seite werden Personen mit keinerlei Berechtigung von den Daten separiert.

2.1.4 Zuverlässigkeit

Microsoft definiert sechs Merkmale, welche auf einem System angewandt werden sollen. Diese Qualitätsmerkmale bestehen im Wesentlichen aus den oben genannten Komponenten Verfügbarkeit und Integrität.

1. ausfallsicher
   Das System kann dem Benutzer auch dann Dienste anbieten, wenn eine interne oder externe Unterbrechung stattfindet. (Verfügbarkeit)

2. wiederherstellbar
   Das System kann nach einer benutzerbedingten oder systembedingten Unterbrechung mittels Instrumentation oder Diagnose problemlos wieder ohne Datenverlust in seinen ursprünglichen Zustand zurückgeführt werden. (Verfügbarkeit)

3. kontrolliert
   Das System erfüllt im Bedarfsfall immer korrekt und rasch die Anforderungen an den gewünschten Dienst. (Verfügbarkeit, Integrität)

4. unterbrechungsfrei
   Erforderliche Änderungen und Aktualisierungen unterbrechen den Systembetrieb nicht. (Verfügbarkeit)

5. produktionsbereit
   Das System weist bereits bei der Auslieferung nur ein Minimum an Fehlern auf, wodurch nur eine begrenzte Zahl an vorhersehbaren Aktualisierungen nötig ist. (Verfügbarkeit)

6. berechenbar
   Das System funktioniert wie erwartet bzw. wie vereinbart. Die Funktionalität von früher bleibt weiter erhalten. (Verfügbarkeit, Integrität)
   [14]

2.2 Schutzbedarf

Der Schutz von Daten und Informationsflüssen gehört für die Unternehmen und öffentlichen Einrichtungen von heute zu den heikelsten und wichtigsten Aufgaben. Ständig aktuelle Daten sind ein unerlässliches Gut für Unternehmen und sollten ständig auf dem neuesten Stand sein. Um diese Daten-Updates durchführen zu können, werden möglichst viele Informationen auf Datenträgern persistent gespeichert. Dabei kann sichergestellt werden, dass diese Daten keinem Risiko ausgesetzt sind sondern mittels spezieller Methodik gesichert und verwahrt werden. Andererseits gibt es aber auch Daten, welche nicht oder nur schwach gesichert werden. Dies kann im schlimmsten Fall zum Verlust von Daten und erheblichen Geldbeträgen führen. Grundlegende Sicherheitsmaßnahmen sind mithilfe von geringen Mitteln und Maßnahmen zu erreichen.

Der Schutzbedarf "Hoch"bedeutet, dass für die Abdeckung dieser Schutzkategorien spezielle Maßnahmen ergriffen werden müssen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellte eine Zusammenstellung aus IT-Grundschutz-Vorgehensweisen und IT-Grundschutzkatalogen an, welche die Voraussetzungen für den Einsatz in den unterschiedlichsten Umgebungen darstellt.

Der Trend zur Speicherung aller Arten von Daten gehört genauso zum alltäglichen Leben wie der Computer selbst. Von Vorratsdatenspeicherung bis hin zu Onlinedatenspeicherung vernetzt über den Globus betrifft das Thema fast jeden Menschen. Selbst der Staat setzt bei Speicherung von Patientendaten und Steuerdaten auf Informationsvernetzung und - speicherung.

Um den teilweise öffentlichen Forderung an Konsistenz und Sicherheit nachkommen zu können, muss der Sicherheitsgrad hoch und der Schutzbedarf gedeckt sein. Schutzbedarf selbst ist nicht quantifizierbar - aber das BSI teilt diesen in drei Kategorien:

1. Normal
   Die Schadensauswirkungen sind begrenzt und überschaubar.

2. Hoch
   Die Schadensauswirkungen können beträchtlich sein.

3. Sehr Hoch
   Die Schadensauswirkungen können ein existentiell bedrohliches bzw. katastrophales Ausmaß erreichen. [6]

Die Sicherheit von Daten und Systemen beschränkt sich heute nur auf technische Gegebenheiten sondern umfasst auch die Sicherheit von organisatorischen und personellen Umgebungsvariablen. Bei diesen ist es enorm wichtig, dass man behutsam und mit großer Flexibilität ans Werk geht. Des Weiteren ist es wichtig, dass mit der richtige Umgang mit sensiblen Daten und mit Betriebsvariablen sichergestellt wird.

Für die heutigen Entwicklungsschritte in der Vernetzungstechnologie sind folgende Faktoren prägend:

1. Vernetzung
   Das Phänomen der Vernetzung wurden in den letzten Jahren durch Internet, VoIP und viele andere technische Errungenschaften verstärkt. Die rasante Entwicklung in den letzten zwei Jahrzehnten hat gezeigt, dass heute nicht mehr isoliert und lokal gebunden gearbeitet wird, sondern mit verschiedenen Rechner und Menschen rund um den Globus kommuniziert wird. Die globale Vernetzung bietet viele verschiedene Möglichkeiten für verteiltes Arbeiten. So können etwa verteilte Ressourcen, gemeinsam genutzte Datenbestände und Cloudcomputing zum eigenen Vorteil genutzt werden.

2. IT-Verarbeitung und Durchdringung
   Im Alltag finden wir heute viele IT-Geräte, die uns das Leben leichter machen sollen. Immer kleiner werdende Teile werden in den unterschiedlichsten Bereichen eingesetzt - vom Auto bis hin zur Küche. Der wohl aktuellste Lebensbereich ist jener der Mobiltelefonie. Kaum jemand besitzt keine Mobiltelefon, welches im Laufe der letzten Jahre zu einem integralen Bestandteil der modernen Gesellschaft wurde.

3. Schwindende Netzgrenzen
   Vor wenigen Jahren war die Softwareentwicklung noch in geographisch lokalen Gebieten eingrenzbar. Doch mittlerweile haben sich einige Bewegungen und Firmen formiert, die ihre Softwareentwicklung auf verschiedene Teams an verschiedenen Orten der Welt aufteilen. Somit ergeben sich nicht gegebenenfalls nicht nur finanzielle sondern auch organisatorische Vorteile.
   [16]

2.3 IT-Schutzkataloge

Der Grundschutzkatalog des BSI ist ein Werk einer deutschen Institution, welches internationales Ansehen genießt. Der gesamte Inhalt wird auch in englischer Sprachen angeboten. BSI-Standards enthalten Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit. Das BSI greift dabei Themenbereiche auf, die von grundsätzlicher Bedeutung für die Informationssicherheit in Behörden oder Unternehmen sind und für die sich national oder international sinnvolle und zweckmäßige Herangehensweisen etabliert haben. Einerseits dienen BSI-Standards zur fachlichen Unterstützung von Anwendern der Informationstechnik. Das erleichtert die sichere Nutzung von Informationstechnik, da auf bewährte Methoden, Prozesse oder Verfahren zurückgegriffen werden kann. [5]

Auszug auf den Grundschutzstandards:

1. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
2. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
3. BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
4. BSI-Standard 100-4: Notfallmanagement

2.4 Aufbau

In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme empfohlen. Ziel des IT-Grundschutzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen. Darüber hinaus bilden die Maßnahmen der IT-Grundschutz-Kataloge nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern liefern an vielen Stellen bereits höherwertige Sicherheit.
Die IT-Grundschutzkataloge sind als Informationssystem-Management organisiert und bestehen aus Bausteinen, welche dem Ganzen eine Struktur geben.

Quelle hinzufügen

2.5 Bausteine

Wie schon vorher erwähnt, bestehen die IT-Grundschutzkataloge aus Bausteinen. Modular kann man sich damit für sich das jeweilige Risikoeinschätzung mit Maßnahmenempfehlungen zusammenbauen. Bausteine werden wie folgt kategorisiert:

- B 1: Übergreifende Aspekte
- B 2: Infrastruktur
- B 3: IT-Systeme
- B 4: Netze
- B 5: Anwendungen

Quelle hinzufügen

Des Weiteren finden sich Bausteine in Gefährdungskatalogen, welche verschiedene Gefährdungsszenarien beschreiben und wie folgst lauten:

- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliches Fehlverhalten

- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen

Quelle hinzufügen

Welche Maßnahmen und Normen einzuhalten sich um das Sicherheitslevel zu erhöhen, beschreiben die nachfolgenden sechs Punkte im Maßnahmenkatalog:

- M 1: Infrastruktur
- M 2: Organisation
- M 3: Personal
- M 4: Hardware und Software
- M 5: Kommunikation
- M 6: Notfallvorsorge

Quelle hinzufügen

2.6 Firewalls

2.6.1 Sicherheitsdienste einer Firewall

2.6.2 Firewall-Konzepte

3 Grundlagen von VoIP

3.1 Geschichte der Telefonie

3.2 Einführung in VoIP

3.3 Technische Grundlagen einer VoIP-Infrastruktur

3.3.1 Protokolle und Standards

3.3.2 Anforderungen an die technische Infrastruktur

3.3.3 Komponenten

3.4 Fallbeispiel: Exemplarischer Aufbau einer VoIP-Infrastruktur

4 Angriffe auf VoIP

4.1 Überblick über die häufigsten Sicherheitsprobleme

4.2 Detaillierte Angriffsschemata

4.2.1 IP-basierte Schwachstellen

4.2.1.1 DoS

4.2.1.2 Flooding

4.2.1.3 Umleitungen

4.2.1.4 Datenmanipulation

4.2.2 Weitere Schwachstellen

4.2.2.1 Eavesdropping

4.2.2.2 ARP-Poisoning

4.2.2.3 SIP Proxy Angriffe

4.2.2.4 SIP Phone Angriffe

4.2.2.5 VoIP-Phishing

4.3 Tools für den Angriff auf VoIP

5 Erhöhung der Sicherheit durch VoIP-Firewalls

5.1 Funktionen

5.2 Aufbau und Spezifikationen

6 Fallbeispiel

6.1 Einrichtung der Testumgebung

6.2 Durchführung der Tests und Protokollierung

6.3 Evaluation der Resultate

7 Conclusio und Ausblick

Abbildungsverzeichnis

Tabellenverzeichnis

Liste der Algorithmen

Abkürzungsverzeichnis

BSI Bundesamt für Sicherheit in der Informationstechnik

Z.B. Zum Beispiel

Literatur

[1] H. Abdelnur u. a. “VoIP security assessment: methods and tools”. In: *Proc. 1st IEEE Workshop VoIP Management and Security*. 2006, S. 29–34.

[2] Z. Anwar u. a. “Multiple design patterns for voice over IP (VoIP) security”. In: *Proc. 25th IEEE Int. Performance, Computing, and Communications Conf. IPCCC 2006*. 2006.

[3] BSI. *BSI Begriffsdefinitionen*.

[4] BSI. *IT-Grundschutz - Basis für Informationssicherheit*.

[5] BSI. *IT-Grundschutz-Kataloge*.

[6] BSI. *Schutzbedarfskategorien*.

[7] D. Butcher, X. Li und J. Guo. “Security Challenge and Defense in VoIP Infrastructures”. In: 37.6 (2007), S. 1152–1162.

[8] X. Cao u. a. “Developing a multifunctional network laboratory for teaching and re- search”. In: *SIGITE ’09: Proceedings of the 10th ACM confer- ence on SIG-information technology education* 2009 (2009), S. 155 –160.

[9] E. Coulibaly und L. Liu. “Security of Voip networks”. In: *Proc. 2nd Int Computer Engineering and Technology (ICCET) Conf.* Bd. 3. 2010.

[10] C. Eckert. *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Oldenbourg Wissensch.Vlg, 2009. ISBN: 9783486589993. URL: http://books.google.com/books?id=akxvOu7pY40C.

[11] C. Egger und M. Hirschbichler. “VoIP Security”. In: *Linux Magazin - Technical Review, Security* 10 (2008), S. 54 –61.

[12] D. Endler und M. Collier. *Hacking exposed VoIP: voice over IP security secrets & solutions*. Hacking Exposed. McGraw-Hill, 2006. ISBN: 9780072263640. URL: http://books.google.com/books?id=IPp07U0OktkC.

[13] E. Eren und K.O. Detken. *VoIP Security: Konzepte und Lösungen für sichere VoIP-Kommunikation*. Hanser Fachbuchverlag, 2007. ISBN: 9783446410862. URL: http://books.google.com/books?id=v8nE9ETF_2kC.

[14] Microsoft Deutschland GmbH. *Die 6 Merkmale der Zuverlässigkeit*.

[15] P. C. K. Hung und M. Martin. “Security Issues in VOIP Applications”. In: *Proc. Canadian Conf. Electrical and Computer Engineering CCECE ’06*. 2006, S. 2361–2364.

[16] Bundesstelle für Informationstechnik. *Glossar*.

[17] T. Porter und T. Porter. *Practical VoIP security*. Syngress Publishing, 2006. ISBN: 9781597490603. URL: http://books.google.com/books?id=BYxdyekyRlwC.

[18] Z. Qu und W. Yang. “The Design of an Active VoIP Security Defense Model Based on Dynamic Self-Adaptive Diffluence”. In: *Proc. Int. Conf. Environmental Science and Information Application Technology ESIAT 2009*. Bd. 1. 2009, S. 657–660.

[19] M. Ronniger u. a. “A robust and flexible test environment for VoIP security tests”. In: *Proc. Int Internet Technology and Secured Transactions (ICITST) Conf. for*. 2010, S. 1–6.