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, 25. Juli 2012

Todo list

Kurzfassung

Über diese Vorlage: Dieses Template dient als Vorlage für die Erstellung einer wissenschaftlichen Arbeit am INSO. Individuelle Erweiterungen, Strukturanpassungen und Layout-Veränderungen können und sollen selbstverständlich nach persönlichem Ermessen und in Rücksprache mit Ihrem Betreuer vorgenommen werden.

Über den Aufbau der Kurzfassung: In der Kurzfassung werden auf einer 3/4 bis maximal einer Seite die Kernaussagen der Arbeit zusammengefasst. Dabei sollte zunächst die Motivation / der Kontext der vorliegenden Arbeit dargestellt werden, und dann kurz die Frage- / Problemstellung erläutert werden, max. 1 Absatz! Im nächsten Absatz auf die Methode / Verfahrensweise / das konkrete Fallbeispiel eingehen, mit deren Hilfe die Ergebnisse erzielt wurden. Im letzten Absatz die Ergebnisse der Arbeit beschreiben.

Wichtig: Verständlichkeit! Die Kurzfassung soll für Leser verständlich sein, denen das Gebiet der Arbeit fremd ist. Deshalb Abkürzungen immer zuerst ausschreiben, in Klammer dazu die Erklärung: z.B: “Im Rahmen der vorliegenden Arbeit werden Non Governmental-Organisationen (NGOs) behandelt, . . . ”

Schlüsselwörter

Schlüsselwörter, wichtig, ThemaMeinerArbeit, Arbeitsgebiet.

Abstract

About this template: This template helps writing a scientific document at INSO. Users of this template are welcome to make individual modifications, extensions, and changes to layout and typography in accordance with their advisor.

Writing an abstract: The abstract summarizes the most important information within less than one page. Within the first paragraph, present the motivation and context for your work, followed by the specific aims. In the next paragraph, describe your methodology / approach, and / or the specific case you are working on. The third paragraph describes the results and the contribution of your work.

Comprehensibility: People with different backgrounds who are novel to your area of work should be able to understand the abstract. Therefore, acronyms should only be used after their full definition has given. E.g., "This work relates to non-governmental organizations (NGOs), . . . ".

Keywords

Keyword, important, SubjectOfMyPaper, FieldOfWork.

Inhaltsverzeichnis

1 Einleitung

1.1 Zielsetzung

Voice over IP (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.
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 (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 und Martin [14] beschrieben werden.

1.2 Aufbau und Methodik

Ziel dieser Arbeit ist die Erläuterung von Möglichkeit zur Absicherung einer VoIP-Infrastruktur, in welcher spezielle VoIP-Firewalls verwendet werden sowie die Darstellung von relevanten Problemen im Bereich von VoIP. Darauf aufbauend sollen Lösungsmuster dargestellt und analysiert werden.

Es sollen bestehende und „vererbte“ Probleme demonstriert und mit Lösungsmöglichkeiten bzw. Abhilfen versehen werden. Konkret wird auf die Fragestellung eingegangen, wie sich eine IT-Landschaft mit VoIP-Einsatz gegen gegenwärtige Probleme (wie z.B. DoS, 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 Standpunkten 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.

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.

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.

1.3 State of the Art

In den vergangenen zehn Jahren haben Sprachkommunikation aus dem Telefonnetz ins Internet verschoben. [24] Die Internet Engineering Task Force (IETF) hat diesen Übergang ermöglicht durch die Entwicklung von stabilen Standards für Anruf-Setup und Medien-Transport. Diese Arbeit soll einen Überblick über diese Standards zeigen, wie sie zusammenarbeiten und wie sie eine vollständige, internetbasierte Echtzeitkommunikation bieten.
Das Internet ist heute sehr vielfältig. Netzwerkfirewalls sind grundlegende Netzwerk-Sicherheitsausrüstungen geworden. Um VoIP-Netzwerk-Umgebung im Normalbetrieb eine Firewall zu ermöglichen, hat die IETF der VoIP-Industrie einige Lösungen vorschlagen [16]. Auf ein paar davon wird in späteren Kapiteln eingegangen.
Ein wichtiger Standard ist Session Initiation Protocol (SIP) [22]. Voice over IP ist eine Technologie, die Sprachdienste und Kommunikation über IP-basierte Netzwerke bietet. SIP erfuhr viel Aufmerksamkeit in den letzten Jahren und ist ein IETF Signalisierungsprotokoll für Session-Management für Text und Multimedia-Austausch, wie VoIP, instant-messaging, Video, Online-Spiele und andere Dienste.

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. [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 [21], 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 Bundesamt für Sicherheit in der Informationstechnik (BSI)- eingehalten werden und sich Mechanismen einbetten lassen, die gegen Angriffe wirksam sind.

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. [11], Eren et al. [13] und Porter [17] beschreiben 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 Integrität

Unter der Integrität (integrity) [15] von Informationen versteht man die Vollständigkeit und Korrektheit (Unversehrtheit) der übertragenen Daten auf Sender- und auch Empfängerseite [4]. 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 [2]. 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.

2.1.2 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.

2.1.3 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.

Ergänzung: 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)

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 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: [6]

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.

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: [15]

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.

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 [3]: Managementsysteme für Informationssicherheit (ISMS)
   Der vorliegende BSI-Standard definiert allgemeine Anforderungen an ein ISMS.

2. BSI-Standard 100-2 [3]: IT-Grundschutz-Vorgehensweise
   Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Sicherheitsmanagements und der Aufbau von Organisationsstrukturen für Informationssicherheit sind dabei wichtige Themen.

3. BSI-Standard 100-3 [3]: Risikoanalyse auf der Basis von IT-Grundschutz
   Die IT-Grundschutz-Kataloge des BSI enthalten Standard-Sicherheitsmaßnahmen aus den Bereichen Organisation, Personal, Infrastruktur und Technik, die bei normalen Sicherheitsanforderungen in der Regel angemessen und ausreichend zur Absicherung von typischen Geschäftsprozessen und Informationsverbünden sind.

4. BSI-Standard 100-4 [3]: Notfallmanagement
   Mit dem BSI-Standard 100-4 wird ein systematischer Weg aufgezeigt, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, um die Kontinuität des Geschäftsbetriebs sicherzustellen. Aufgaben eines Notfallmanagements sind daher, die Ausfallsicherheit zu erhöhen und die Institution auf Notfälle und Krisen adäquat vorzubereiten, damit die wichtigsten Geschäftsprozesse bei Ausfall schnell wieder aufgenommen werden können.

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

Bausteine
Der Bausteinkatalog ist ein zentrales Element für den Schutz. Dieser besteht aus einem Schichtenmodell, so wie auch die weiteren Kataloge. Wie in Kapitel 2.4 beschrieben, bestehen die IT-Grundschutzkataloge aus Bausteinen. Modular kann man sich damit die 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

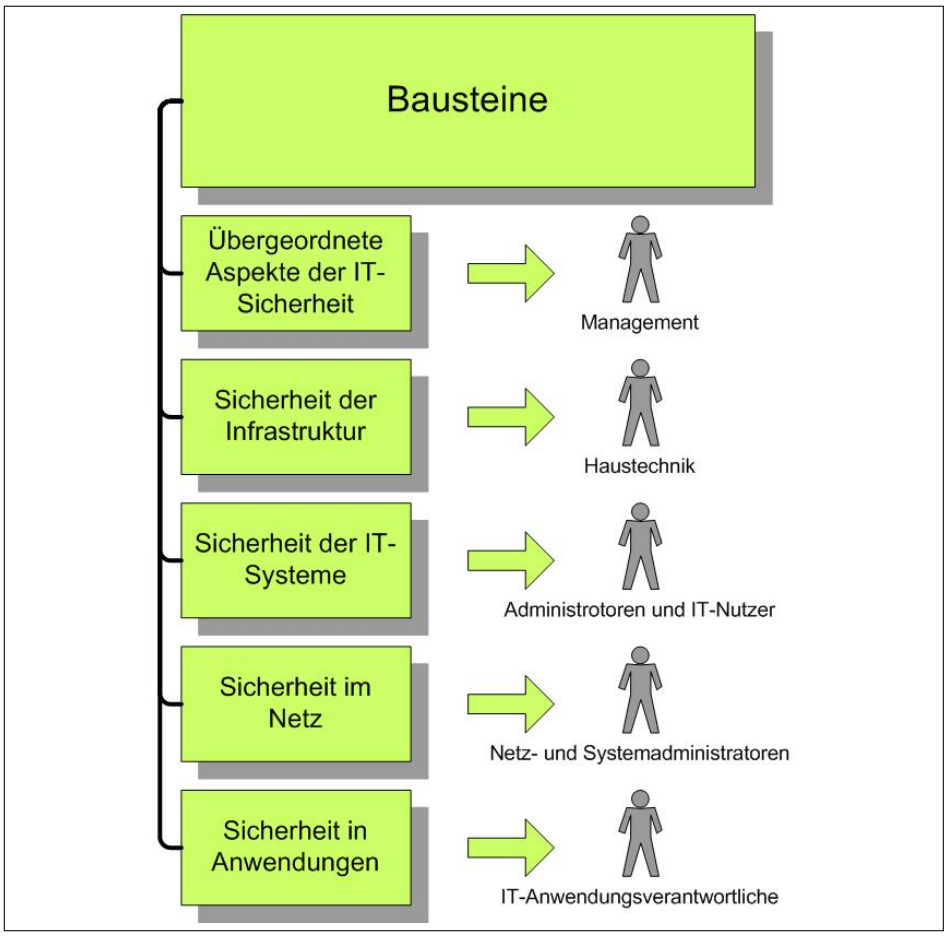

Abbildung 2.1: Bausteinzuordnung-BSI-Grundschutzkataloge

Quelle Wikipedia hinzufügen

Die erste Schicht beschäftigt sich mit organisatorischen Fragen das Management, Personal oder Outsourcing betreffend. In der Schicht Infrastruktur wird der Schwerpunkt auf bauliche Aspekte gelegt. Die Schicht IT-Systeme befasst sich mit den Eigenschaften von IT-Systemen zu denen neben den Clients und Servern auch Telefonanlagen oder Faxgeräte gezählt werden. In der Netze-Schicht werden Aspekte von Netzwerken beleuchtet. Die Anwendungsschicht befasst sich mit Fragen sicherheitsrelevanter Software wie Datenbankmanagementsystemen, E-Mail oder Webservern. Durch die Einteilung in Schichten lassen sich auch die von der jeweiligen Schicht betroffenen Personengruppen klar eingrenzen. Die erste Schicht spricht das Management an. Haustechniker sind von der zweiten betroffen. Die dritte Schicht wird von Systemadministratoren abgedeckt. Die vierte Schicht fällt in den Aufgabenbereich der Netzwerkadministratoren und die fünfte in den der Anwendungsadministratoren und der IT-Nutzer. Jeder einzelne Baustein folgt demselben Aufbau. Die Bausteinnummer setzt sich zusammen aus der Nummer der Schicht in dem sich der Baustein befindet und einer in dieser Schicht eindeutigen Nummer. Nach einer kurzen Beschreibung des vom Baustein betrachteten Sachverhalts wird die jeweilige Gefährdungslage geschildert. Anschließend folgt die Aufzählung der einzelnen Gefahrenquellen. Diese stellen eine weiterführende Information dar und sind für die Erstellung eines Grundschutzes nicht notwendigerweise durchzuarbeiten.

Die notwendigen Maßnahmen werden mit kurzen Erläuterungen in einem Text vorgestellt. Der Text folgt hierbei dem Lebenszyklus des jeweiligen Sachverhalts und umfasst Planung und Konzeption, Beschaffung (falls erforderlich), Umsetzung, Betrieb, Aussonderung (falls erforderlich) und Notfallvorsorge. Nach der ausführlichen Schilderung werden die einzelnen Maßnahmen nochmals in einer Liste zusammengefasst, die jedoch nun nach der Struktur der Maßnahmenkataloge und nicht mehr nach dem Lebenszyklus sortiert ist. Hierbei wird eine Klassifizierung der Maßnahmen in die Kategorien A, B, C, Z und W vorgenommen. Maßnahmen der Kategorie A bilden den Einstieg in die Thematik, B-Maßnahmen erweitern diese und die Kategorie C ist anschließend notwendig für eine Zertifizierung des Grundschutzes. Maßnahmen der Kategorie Z stellen zusätzliche Maßnahmen dar, die sich in der Praxis bewährt haben. Maßnahmen der Kategorie W sind Maßnahmen die Hintergrundwissen zum jeweiligen Thema liefern und für ein zusätzliches Grundverständnis der jeweiligen Thematik beitragen.

Quelle Wikipedia hinzufügen, Formulierung!

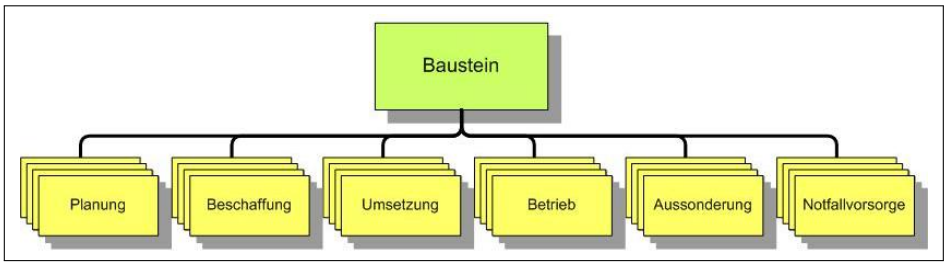

Abbildung 2.2: Lebenszyklus-BSI-Grundschutzkataloge

Quelle Wikipedia 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

Die Gefährdungskataloge gehen näher auf die möglichen Gefährdungen für IT-Systeme ein. Diese Gefährdungskataloge folgen dem allgemeinen Aufbau nach Schichten. Zur Erstellung des Grundschutzes ist nach Aussagen des BSI das in diesen Katalogen zusammengestellte Wissen nicht unbedingt notwendig, es fördert jedoch das Verständnis für die Maßnahme sowie die Wachsamkeit der Verantwortlichen. Die einzelne Gefahrenquelle ist in einem kurzen Text beschrieben und anschließend werden Beispiele für Schadensfälle, die durch diese Gefahrenquelle auslösen kann, gegeben.

Quelle hinzufügen

Quelle=Wikipedia hinzufügen

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

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

Die zur Umsetzung des Grundschutzes notwendigen Maßnahmen sind in Maßnahmenkatalogen zusammengefasst. So werden Maßnahmen, die für mehrere System-Komponenten angemessen sind, nur einmal zentral beschrieben. Hierbei werden auch Schichten zur Strukturierung der einzelnen Maßnahmengruppen genutzt. In der jeweiligen Maßnahmenbeschreibung sind zunächst Verantwortliche für die Initiierung und die Umsetzung der Maßnahme genannt. Es folgt eine ausführliche Beschreibung der Maßnahme. Abschließend werden Kontrollfragen zur korrekten Umsetzung genannt. Bei der Umsetzung der Maßnahmen sollte zunächst überprüft werden, ob eine Anpassung dieser auf den jeweiligen Betrieb notwendig ist. Eine genaue Dokumentation solcher Anpassungen ist zur späteren Nachvollziehbarkeit sinnvoll. Am Ende der Maßnahmen gibt es seit der 10. Ergänzungslieferung sogenannte Prüffragen, die die wesentlichen Aspekte einer Maßnahme nochmal aufgreifen und somit eine Art Checkliste darstellen, ob diese auch umgesetzt sind.

Quelle=Wikipedia hinzufügen

Quelle hinzufügen

Weiters gibt der IT-Grundschutzkatalog

Quelle hinzufügen

wertvolle Hinweise, um theoretisch und praktisch einen effektiven Sicherheitsprozess zu gewährleisten.

2.4 Firewalls

Das BSI hat sicherheitsspezifische Aspekte für Firewalls beschrieben. Sicherheitsspezifische Funktionen sind alle Funktionen einer Firewall, die direkt zum Erreichen der Sicherheitsziele beitragen.

Sicherheitsrelevante Funktionen tragen zum sicheren Funktionieren der Firewall bei und leisten häufig nicht nur Dienste für die sicherheitsspezifischen Funktionen, sondern auch für nicht sicherheitsbezogene Funktionen. Für gewöhnlich hängen sicherheitsspezifische Funktionen vom korrekten Betrieb der sicherheitsrelevanten Funktionen ab. Sicherheitsrelevante Funktionen sind alle Bestandteile, die für die Ausführung der sicherheitsspezifischen Funktionen benötigt werden, also z.B. Teile des Betriebssystems wie Netzwerktreiber, Bibliotheksfunktionen o.Ä. Sie müssen also auch gemäß der oben aufgeführten Evaluationsstufen geprüft werden, wobei auch Wechselwirkungen zu berücksichtigen sind! Zur Erreichung einer größtmöglichen Vereinfachung und Standardisierung sollten die sicherheitsrelevanten Funktionen über eine kleine Anzahl von genau definierten Schnittstellen angesprochen werden können. Die sicherheitsspezifischen Funktionen einer Firewall lassen sich wie folgt unterteilen:

- Funktionen zum Schutz gegen direkte Angriffe
- Funktionen zum Schutz des zu sichernden Netzes gegen Angriffe aus dem unsicheren Netz

Quelle hinzufügen

2.4.1 Sicherheitsdienste einer Firewall

Auf dem Firewall-System werden Sicherheitsmechanismen implementiert, die diesen Übergang sicher und beherrschbar machen. Dazu analysiert das Firewall-System die Kommunikationsdaten, kontrolliert die Kommunikationsbeziehungen und Kommunikationspartner, reglementiert die Kommunikation nach einer Sicherheitspolitik, protokolliert sicherheitsrelevante Ereignisse und alarmiert bei starken Verstößen den Security-Administrator.

Allgemeine Ziele von Firewall-Systemen

- Zugangskontrolle: Auf Daten-, Benutzer- und Netzwerkebene kann die Sicherheit überprüft und gewährleistet werden, damit ein sicherer Datenaustausch möglich ist.
- Rechteverwaltung: Mittels Protokollen und Diensten kannst festgelegt werden, wann für wen eine Kommunikation über das Firewall-System erlaubt ist.
- Vertraulichkeit: Die interne Struktur wird hinter dem Schutzsystem verborgen und Nachrichten werden nie im Klartext übermittelt.

Quelle hinzufügen

Nachfolgende Grafik zeigt die exemplarische Einbindung einer Firewall in ein Netzwerk und die Platzierung einer Firewall.

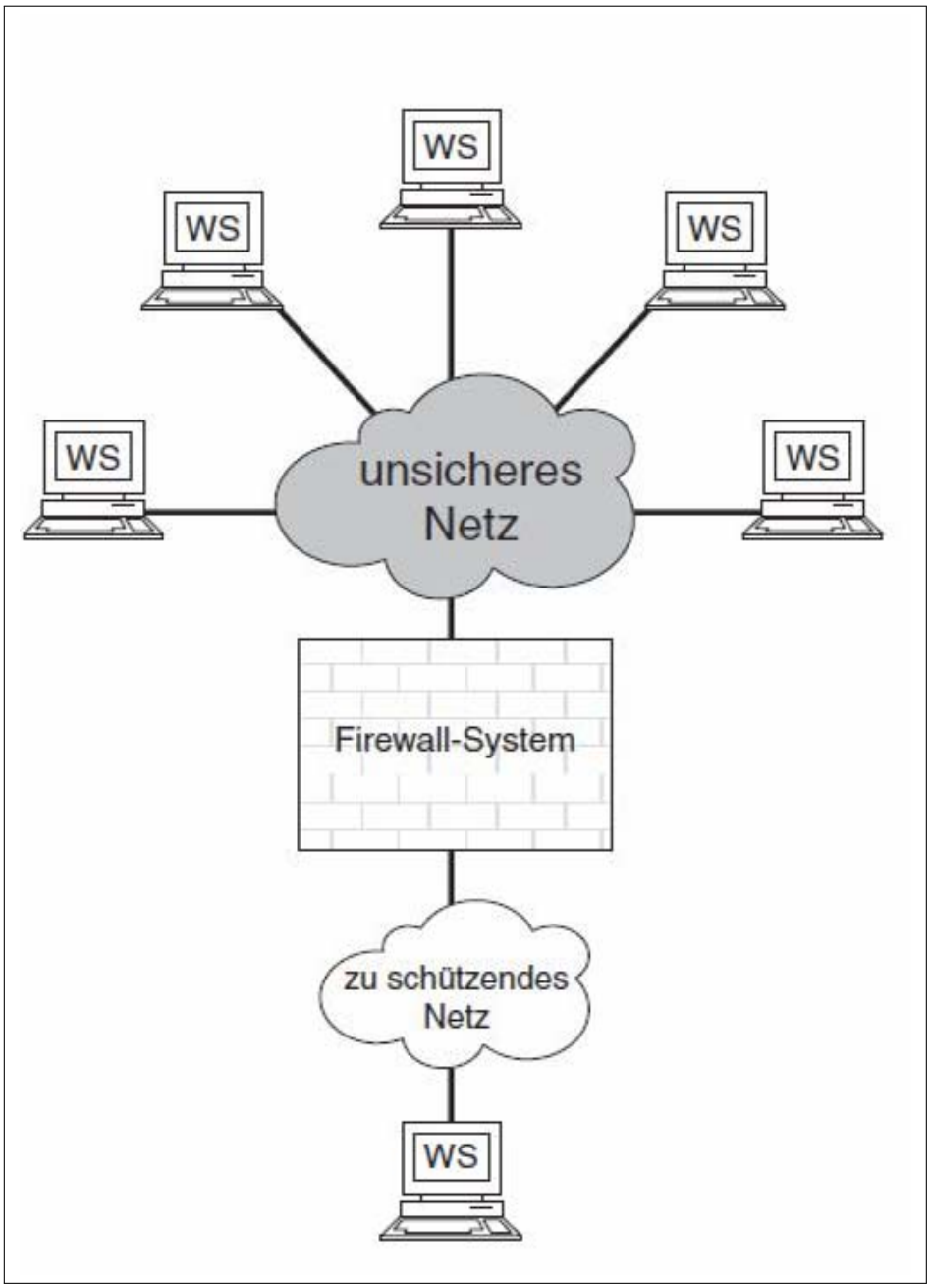

Abbildung 2.3: Firewall-Network

Quelle hinzufügen

2.4.2 Firewall-Konzepte

Ein Firewall-System stellt den "Common Point of Trust"für den Übergang zwischen unterschiedlichen Netzen dar, d.h., der einzige Weg ins interne Netz führt kontrolliert über das Firewall-System. Firewall-Systeme werden verwendet, um sich an unsichere Netze wie z.B. das Internet anzukoppeln oder auch, um das eigene Netz zu strukturieren und hier Sicherheitsdomänen mit unterschiedlichem Schutzbedarf zu schaffen.

Quelle hinzufügen

Vorteile des Common-Point-of-Trust-Konzeptes

- Kosten: Die Realisierung von Sicherheitsmechanismen auf einem zentralen System ist wesentlich einfacher jene auf jedem einzelnen Rechner.
- Möglichkeiten durch Sicherheitspolitik: Durch eine zentrale Steuerung können die Benutzer einheitlich authentifiziert werden und womöglich mit kryptographischen Funktionen erweitert werden.
- Abschottung: Durch diese Konzeptionierung kann das zu schützende Netzwerk von unsicheren Netzwerken getrennt werden. Firewall-Systeme können Angriffen entgegenwirken.

Quelle hinzufügen

Screened Subnet [20]

Das Screened Subnet ist ein entkoppeltes, isoliertes Teilnetzwerk, das zwischen das interne und das unsichere Netz geschaltet wird. In diesem Teilnetzwerk überprüfen zwei Packet Filter die Datenpakete aus dem internen und dem externen Netz, ein oder mehrere Informationsserver stellen dem öffentlichen Netz Informationen zur Verfügung, und in der Bastion werden die Informationen auf der Anwendungsschicht kontrolliert.

Dem unsicheren Netz sind nur die Rechner im Screened Subnet bekannt, die Rechner des zu schützenden Netzes bleiben verborgen.

Packet Filter [20]

Die beiden Packet Filter bilden den Zugang zum Screened Subnet. Der Sicherheitsmechanismus Packet Filter analysiert die ein- und ausgehenden Netzwerk-Frames. Dabei werden die Filterregeln so definiert, dass jede IP-Verbindung von innen (zu schützendes Netz) und außen (unsicheres Netz) über die Bastion geroutet wird. Für nicht auf IP basierende Protokolle, wie z.B. Open Systems Interconnection (OSI), können die Filterregeln der beiden Packet Filter so definiert werden, dass die Pakete direkt zwischen ihnen geroutet werden.
Dabei wird im IP-Header die Source- und Destination-Adresse kontrolliert. Es wird überprüft, ob die Verbindung mit Hilfe von UDP oder TCP durchgeführt wird, und wer die Verbindung aufbaut. Außerdem werden die Dienste/Portnummern (FTP, Telnet, HTTP usw.) kontrolliert. Die Informationen darüber, was zu überprüfen ist, werden einer Rechteliste (Access List) entnommen. Bei Verstoß gegen die Regeln wird dies entsprechend protokolliert und, falls definiert, eine Warnmeldung an das Security Management gesendet.

Application Gateway [20]

Ein Application Gateway ist ein Computer mit einem sicheren Betriebssystem und i.d.R. zwei Netzwerkanschlüssen, der die beiden Netzbereiche logisch und physikalisch entkoppelt. In der Bastion werden die Informationen auf der Anwendungsschicht kontrolliert und eine Benutzerauthentikation durchgeführt.
Als einziger vom unsicheren Netz (z.B. Internet) erreichbarer Host muss der Application Gateway besonders geschützt werden. Die Benutzer, die über die Bastion auf Rechnersysteme im zu schützenden Netz zugreifen möchten, müssen zuerst eine Identifikation und Authentikation mit der Bastion durchführen, wozu spezielle Passwortsysteme (Einmalpasswort, Sicherheitstoken) eingesetzt werden.
Auf dem Application Gateway wird für jeden erlaubten Dienst (Telnet, FTP usw.) ein sogenannter Proxy Agent installiert, der spezielle Sicherheitsfunktionen zur Verfügung stellt. Das bedeutet, dass über die Bastion nur Dienste verwendet werden können, für die entsprechende Proxy Agents installiert wurden. Für den FTP-Proxy Agent kann dann z.B. definiert werden, welcher Befehl verwendet werden darf und welcher nicht.

Der Proxy Agent nimmt eine Verbindung vom Quellrechner an, baut nach der Überprüfung der Quell- und Zieladresse eine Verbindung zum Zielrechner auf und transferiert dann Datenpakete zwischen diesen Verbindungen. Außerdem werden die Aktivitäten, die über die Bastion abgewickelt werden, protokolliert, z.B. welche Dateien mit welchen Attributen übertragen werden.
Auf der Bastion selbst dürfen keine unnötigen bzw. nicht unbedingt notwendigen Prozesse im Hintergrund laufen, die häufig die Ursache von Sicherheitslücken sind.

Security Management Station [20]

Mit Hilfe des Security Managements werden die Zugangskontrolltabellen verwaltet und in die Packet Filter sowie in den Application Gateway geladen. Die Logbücher aus den Packet Filtern und der Application Gateway können gelesen und ausgewertet werden. Weiterhin versorgt das Security Management die Packet Filter und die Application Gateway mit den benötigten sicherheitsrelevanten Informationen, zum Beispiel mit Schlüsseln. Dabei ist die Kommunikation zwischen den Packet Filtern sowie mit der Bastion und dem Security Management kryptographisch gesichert. Die Logbücher können bei Bedarf (z.B. bei einem Angriffsversuch) zur Beweissicherung verwendet werden.

Information Server [20]

Informationen, die öffentlich zugänglich sein sollen, werden auf einem Information Server dem Internet zur Verfügung gestellt. Dieser Information Server steht vor der Application Gateway. Damit ist ein Zugriff von außen auf das zu schützende Netz nicht möglich.
Durch die Entkopplung der Netze gelangen User aus dem unsicheren Netz nur bis zum Information Server, der sich vor der Bastion befindet, nicht jedoch unkontrolliert durch sie hindurch.

Formatierung!

3 Grundlagen von VoIP

Allgemein gesprochen beschreibt Voice over IP die Telefonie basierend auf dem Transmission Control Protocol/Internet Protocol (TCP/IP) Protokoll im Internet.

Mit VoIP werden mehrere Begriffe verbunden; z.B.:

- Internet Protocol (IP)-Telefonie
- Skype
- Local Area Network (LAN)-Telefonie
- SIP-Telefonie
- Internettelefonie

3.1 Geschichte der Telefonie

Kommunikation ist ein Grundbedürfnis aller Menschen. Allein wie die Information übermittelt wird, hat sich im Laufe der Geschichte immer wieder geändert. Seit Jahrzehnten ist das Telefon fester Bestandteil unseres Lebens. Der Griff zum Hörer, der Gespräche mit Menschen rund um die Welt ermöglicht, ist heute eine Selbstverständlichkeit. Vor 12 Jahren, als die Geschichte der Telefonie in Österreich begann, war das Telefon jedoch eine sensationelle Innovation.

Im Juni des Jahres 1881 erteilte das k.k. Handelsministerium der "Wiener Privat-Telegraphen-Gesellschaftëine "Concessionßum Betrieb von Telefonanlagen. Zwar erscheint die Netzabdeckung aus heutiger Sicht wenig beeindruckend, die Telefonanlagen durften lediglich in einem Umkreis von 15 Kilometern rund um den Wiener SStephansthurm"betrieben werden. Schon drei Monate später wurde der Betrieb der Telefonanlagen auf ganz Wien ausgeweitet, im Dezember 1881 konnte in der Wiener Friedrichstraße die erste Telefonzentrale Österreichs eröffnet werden. Mit 154 Teilnehmern, darunter Zeitungen, Großunternehmer und Banken, wurde der Netzbetrieb gestartet.

Im Jahr 1867 entwickelte Alexander Graham Bell eine Versuchsanordnung, bei der Schallwellen der menschlichen Sprache eine Membran vibrieren ließen. Dadurch entstanden in einer Drahtspule Stromschwankungen, die nach der Übertragung auf ein gleichartiges Gerät wieder Töne hervorbrachten. Bell erhielt für seine Erfindung die Patentnummer 174.465 und war damit nur um zwei Stunden schneller als der Amerikaner Elisha Gray. Damals konnte noch niemand ahnen, dass die Erfindung zu einem der einträglichsten Patente aller Zeiten werden sollte. Im Jahr 1876 wurde über den "Bellschen Sprachtelegraphenßchließlich zwischen Boston und Cambridge das erste Ferngespräch der Welt geführt.

Im Jahre 1910 kamen schließlich die ersten Telefone, die mit einer Wählscheibe und einem Hörer ausgestattet waren, auf den Markt. Zugleich bereitete die Post- und Telegraphenverwaltung mit der Umstellung der Verbindungen innerhalb eines Ortes vom handvermittelten Dienst auf Selbstwählverkehr eine kleine Revolution vor. Nun konnten die Teilnehmer erstmals ihre Gesprächspartner innerhalb eines Ortes direkt und ohne Vermittlungshilfe erreichen. Schon in den Anfangsjahren der Telefonie gab es Verbindungen in die österreichischen Kronländer. Allerdings wurden diese Leitungen bis etwa 1920 ausnahmslos über Freileitungstrassen geführt.

[23]

3.2 Einführung in VoIP

Mit der Thematik Voice over IP hat die Telefonie einen riesen Schritt vorwärts getan. Durch die starke Verbreitung von Smartphones haben sich noch weitere Geschäftsfelder für die Internettelefonie hinzugekommen. Internationale Firmen haben diese Chancen längst erkannt und stellen sich dementsprechend auf.
Basierend auf den Protokollen IP, Transmission Control Protocol (TCP) und User Datagram Protocol (UDP) lässt sich VoIP leicht in bestehende Infrastruktur und Dienste integrieren. Im nächsten Kapitel werden die technischen Details noch näher erläutert.
Firmen nutzen die gleiche Infrastruktur zur Datenübertragung und zur Telefonie. Das brachte viele Vorteile mit sich und somit auch den Durchbruch für VoIP. Herkömmliche Telefonie war davor immer kanalorientiert gewesen. Im Bereich von VoIP spricht man von einer Paketorientierung im Bezug auf die Verbindung.
Eine paketorientierte Übertragung von Sprache nutzt Leitungskapazität gezielter aus als die bisherige Methode einer Reservierung der gesamten Leitung. Durch Effizienz in der Mediumsnutzung und Flexibilität in der Anwendung ergab sich im Laufe der Zeit eine Überlegenheit von VoIP.

Quelle hinzufügen

Als Konsequenz daraus ergibt sich eine hohe Erreichbarkeit. Gebremst werden kann das nur durch die verfügbare Bandbreite, welche sich aber im Laufe der letzten Jahre verbessert hat. Das aufkommende Datenvolumen spielt in seltenen Fällen eine Rolle - wird jedoch von den Providern kritischer gesehen.
Wesentlich für das Zustandekommen von Internettelefonie und Gesprächen ist, dass die analoge Telefonie digital verarbeitet wird. Die Sprache wird in IP-Pakete umgewandelt und in manchen Fällen auch verschlüsselt, um die Sicherheit zu erhöhen.

Quelle hinzufügen

Vorteile von VoIP

- Interne Gespräche ohne Gebühren
- Daten und Sprachübertragung in einem Medium
- Ortsungebundenheit im Gegensatz zum Festnetz
- Kostenersparnis bei Auslandsgesprächen
- Erweiterbarkeit
- Unabhängige Komplettlösung

Nachteile von VoIP

- Sicherheitsrisiko durch Abhängigkeit von Internet
- Qualitätsdefizit möglicherweise durch Hardware und Bandbreite
- Zuverlässigkeit fraglich durch Hardwaredefekt oder Leitungsausfall
- Notrufe nur eingeschränkt möglich
- Stromkosten wesentlich höher

- Externe Abhängigkeit von regionaler Infrastruktur (z.B. Stromnetz)

Quelle hinzufügen

3.3 Technische Grundlagen einer VoIP-Infrastruktur

Bei der Internettelefonie gibt es mehrere Schwerpunkte, die in diesem Kapitel diskutiert werden. Die Kernfragen sind der Transport der Sprache, die Sicherung von Datenströmen und Sprachinformationen und der Medienübergang in angrenzende Systeme.

3.3.1 Protokolle und Standards

RTP und RTCP

H.323

SIP

SIP - STP

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 Conclusio und Ausblick

7 Ergebnisse

Die Resultate der Arbeit präsentieren und nach Möglichkeit aussagekräftige, eigenständige Abbildungen einbauen. Namen des Kapitels konkretisieren, an jeweilige Arbeit anpassen – Lösungsvorschlag/Implementierung im Titel des Kapitels benennen. Bei einer Software-Entwicklungsarbeit ggf. eine Beschreibung der Qualitätsmerkmale der neuen Implementierung (Performance, Sicherheit, Messergebnisse etc.) geben.

Bei einer Arbeit zu einem abstrakteren Architekturthema können hier die Eigenschaften nach der Anwendung der konzipierten Architektur beschrieben werden. Kommt sie in mehreren Fallbeispielen zum Einsatz, erfolgt hier ein Vergleich der jeweiligen Ergebnisse (z.B. gab es Unterschiede im Umsetzungserfolg, die sich auf konkrete Eigenschaften der betrachteten Fallbeispiele zurückführen lassen).

Bei einer Arbeit zur Softwareauswahl und Einführung wird eine Beschreibung von Qualitätseigenschaften des mit der Einführung neu geschaffenen SOLL-Zustands gegeben.

Bei einer Arbeit, deren Fokus auf der Durchführung und Auswertung von Fragebögen liegt, erfolgt in diesem Kapitel die Auswertung der Fragebögen.

8 Zusammenfassung und Ausblick

Die Zusammenfassung ist nach der Kurzfassung der am häufigsten gelesene Teil, da viele Leser aus Zeitknappheit Arbeiten im Schnellverfahren konsumieren und rasch zur Zusammenfassung blättern. Hier hat man die Chance, dem Leser noch einmal die zentralen Ideen und Ergebnisse der Diplomarbeit zu vermitteln.

Im Gegensatz zur Kurzfassung sind die Leser mit der Problemstellung und der Terminologie bereits vertraut. In der Länge hat man deutlich mehr Spielraum als bei der Kurzfassung, die Zusammenfassung sollte inklusive Ausblick 2 bis max. 10 Seiten umfassen. Hier sollten kompakt die Antworten auf die in der Zielsetzung aufgeworfenen Fragen (Hypothesen) gegeben werden.

Neben einer Zusammenfassung der wichtigsten Ergebnisse sollte auch ein Ausblick gegeben werden: Aufzeigen des Bedarfs an zukünftiger Forschung, potentielle Anwendungsmöglichkeiten der vorgestellten Lösung etc.

In Summe sollte die Zusammenfassung dem Leser die wissenschaftliche und, wenn vorhanden, praktische Relevanz der Arbeit klar und verständlich darlegen.

Abbildungsverzeichnis

Tabellenverzeichnis

Quellcodeverzeichnis

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] BSI. *BSI Begriffsdefinitionen*. URL: https://www.bsi.bund.de/cln_183/sid_C6E2892F31C8991A1AAD7D06
ContentBSI/grundschutz/kataloge/glossar/04.html.

[3] BSI. *BSI Grundschutzstandards*. URL: https://www.bsi.bund.de/ContentBSI/Publikationen/
BSI_Standard/it_grundschutzstandards.html.

[4] BSI. *IT-Grundschutz - Basis für Informationssicherheit*. URL: https://www.bsi.bund.de/
DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Allgemeines/Einstiegskapitel/
einstiegskapitel_node.html.

[5] BSI. *IT-Grundschutz-Kataloge*. URL: https://www.bsi.bund.de/cln_174/DE/Themen/
weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html.

[6] BSI. *Schutzbedarfskategorien*. URL: https://www.bsi.bund.de/cln_156/DE/Themen/
weitereThemen/WebkursITGrundschutz/Schutzbedarfsfeststellung/Schutzbedarfskategorien/
schutzbedarfskategorien_node.html.

[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 research”. 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.

[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 and solutions*. Hacking Exposed. McGraw-Hill, 2006. ISBN: 9780072263640.

[13] E. Eren und K.O. Detken. *VoIP Security: Konzepte und Lösungen fü sichere VoIP-Kommunikation*. Hanser Fachbuchverlag, 2007. ISBN: 9783446410862.

[14] 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.

[15] Bundesstelle für Informationstechnik. *Glossar*. URL: http://www.bit.bund.de/cln_092/nn_
2149510/BIT/DE/Zentrale__Dienste/DVDV/Glossar/Functions/glossar,lv2=2149638.
html.

[16] Chung-Hsin Liu und Wu-Fan Hsu. “The Study of the VoIP through Firewall Security”. In: *Multimedia and Information Technology (MMIT), 2010 Second International Conference on*. Bd. 2. Apr. 2010, S. 289 –292. DOI: 10.1109/MMIT.2010.159.

[17] T. Porter und T. Porter. *Practical VoIP security*. Syngress Publishing, 2006. ISBN: 9781597490603.

[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. 96–101.

[20] secupedia.info. *Übersicht Firewall*. URL: http://www.secupedia.info/wiki/Firewall.

[21] S. Strobel. *Firewalls und IT-Sicherheit*. dpunkt-Verl., 2003. ISBN: 9783898641524.

[22] Lu Tian u. a. “Study of SIP protocol through VoIP solution of Asterisk”. In: *Mobile Congress (GMC), 2011 Global*. Okt. 2011, S. 1 –5. DOI: 10.1109/GMC.2011.6103925.

[23] Stadt Wien. *Geschichte des Telefons*. URL: http://www.stadt-wien.at/unternehmen/dienstleistungen/125-jahre-festnetz/zone-1.html.

[24] T. Zourzouvillys und E. Rescorla. “An Introduction to Standards-Based VoIP: SIP, RTP, and Friends”. In: *Internet Computing, IEEE* 14.2 (März 2010), S. 69 –73. ISSN: 1089-7801. DOI: 10.1109/MIC.2010.31.