INSO - Industrial Software
Institut für Rechnergestützte Automation | Fakultät für Informatik | Technische Universität Wien

Exposé zur Bakkalaureatsarbeit

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

Betreuer: Thomas Grechenig
Betreuender Assistent: Florian Fankhauser

Philipp Schaden
0626698
033 526
Wirtschaftsinformatik

11.09.2011

.....
Thomas Grechenig

Exposé zur Bakkalaureatsarbeit

1 Problemstellung

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.

1.2 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. [10]

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 [12] 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.

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.

4 State of the Art

Ronniger et al. stellen in [13] 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 [4] 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 [5], dass der zentrale Punkt einer für diese Arbeit relevanten Testumgebung die VoIP-Firewall bildet. Diese ist laut Coulibaly et al. in [5] speziell ausgerichtet und der zentrale Angriffspunkt des Testnetzwerkes.
Aber laut Butcher et al. in [3] muss auch VoIP-Software auf Schwachstellen getestet werden. Eckert schreibt in [6] 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. [8] unschwer möglich, VoIP-Telefone bzw. das gesamte VoIP-Netzwerk zu hacken.
Egger et al., Eren et al. und Porter beschreiben in [7] ,[9] ,[11] Möglichkeiten, um die richtigen Sicherheitsmaßnahmen für eine gegebene Infrastruktur zu wählen. Weiters soll man sich Vorkenntnisse durch Recherche aneignen und in andere Erfahrungsberichte einlesen.

5 Inhaltsverzeichnis

geplante Struktur der Arbeit:

Gliederung	Thema	Seiten
1	Einleitung	
1.1	Zielsetzung	1
1.2	Aufbau und Methodik	2
2	Grundlagen der IT-Sicherheit	
2.1	Sicherheitsziele	1
2.1.1 - 2.1.3	Integrität, Verfügbarkeit, Vertraulichkeit	3
2.2	Schutzbedarf	2
2.3	IT-Grundschutzkataloge	1
2.4	Firewalls	3
2.4.1	Sicherheitsdienste einer Firewall	3
2.4.2	Firewall-Konzepte	3
3	Grundlagen von VoIP	
3.1	Geschichte der Telefonie	2
3.2	Einführung in VoIP	1
3.3	Technische Grundlagen einer VoIP-Infrastruktur	2
3.3.1	Protokolle und Standards	2
3.3.2	Anforderungen an die technische Infrastruktur	2

3.3.3	Komponenten	2
3.4	Fallbeispiel: Exemplarischer Aufbau einer VoIP-Infrastruktur	1
4	Angriffe auf VoIP	
4.1	Überblick über die häufigsten Sicherheitsprobleme	3
4.2	Detaillierte Angriffsschemata	2
4.2.1	IP-basierte Schwachstellen	2
4.2.1.1 - 4.2.1.4	DoS, Flooding, Umleitungen, Datenmanipulation	2
4.2.2	Weitere Schwachstellen	2
4.2.2.1 - 4.2.2.2	Eavesdropping, ARP-Poisoning	1
4.2.2.3 - 4.2.2.4	SIP Proxy/Phone Angriffe	1
4.2.2.5	VoIP-Phishing	1
4.3	Tools für den Angriff auf VoIP	2
5	Erhöhung der Sicherheit durch VoIP-Firewalls	2
5.1	Funktionen	2
5.2	Aufbau und Spezifikationen	3
6	Fallbeispiel	2
6.1	Einrichtung der Testumgebung	2
6.2	Durchführung der Tests und Protokollierung	2
6.3	Evaluation der Resultate	3

6 Zeitplanung

1. Expose Abgabe: 07.09.
2. Praktikum: November
3. Abgabe erstes Konzept der Arbeit: Ende November

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. DOI: 10.1109/VOIPMS.2006.1638119.

[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. DOI: 10.1109/.2006.1629443.

[3] D. Butcher, Xiangyang Li und Jinhua Guo. “Security Challenge and Defense in VoIP Infrastructures”. In: 37.6 (2007), S. 1152–1162. DOI: 10.1109/TSMCC.2007.905853.

[4] 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.

[5] E. Coulibaly und Lian Hao Liu. “Security of Voip networks”. In: *Proc. 2nd Int Computer Engineering and Technology (ICCET) Conf.* Bd. 3. 2010. DOI: 10.1109/ICCET.2010.5485790.

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

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

[8] 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.

[9] 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.

[10] Patrick C. K. Hung und Miguel Vargas Martin. “Security Issues in VOIP Applications”. In: *Proc. Canadian Conf. Electrical and Computer Engineering CCECE ’06*. 2006, S. 2361–2364. DOI: 10.1109/CCECE.2006.277789.

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

[12] Zhaoyang Qu und Wei 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. DOI: 10.1109/ESIAT.2009.88.

[13] 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.