IT Sicherachitekturen

Einrichtung einer internen Firewall von Firma-a und Firma-b, sowie LAN-to-LAN-VPN von Firma-a (Server) nach Firma-b(Client)

Paul Drautzburg Georg Mohr

HTWG Konstanz, Sommersemester 2018

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Motivation

Im Zeitalter der Digitalisierung steigt der Grad der Vernetzung immer weiter an. Unternehmen, welche ihre Standorte über die ganze Welt verteilt haben, wollen Wege und Möglichkeiten haben ihre Arbeit sicher und Problemlos zu verrichten. Dafür ist es unerlässlich, dass verschiedene Standorte auf Ressourcen des anderen zugreifen können. Für solche Szenarien gibt es in der Netzwerktechnik und Netzwerkarchitektur verschiedene Lösungsansätze. Jedoch darf dabei ein wichtiger Aspekt nicht vernachlässigt werden, denn jedes Unternehmen hat Betriebsmittel und Informationen, welche es nicht Gefahren von außen aussetzten will. An diesem Punkt kommt der Begriff IT-Sicherheit ins Spiel und genau dieses Umfeld um den Begriff „IT-Sicherheit“ wird im Rahmen des Praktikums zur Lehrveranstaltung „IT-Sicherheitsarchitekturen“ untersucht. In den folgenden Kapiteln wird eine Problemstellung unter Laborbedingungen skizziert, welche ein Szenario wiederspiegelt, mit dem sich Unternehmen täglich konfrontiert sehen. Anschließend wird werden die Laborbedienungen und der Versuchsaufbau beschrieben. Aus der Problemstellung und dem Versuchsaufbau wird eine Lösung auf Grundlage, der damit zu Grunde liegenden Theorie, erarbeitet. Diese Lösung wird abschließend in die Laborumgebung implementiert und auf ihre Akzeptanz gegenüber der Problemstellung untersucht und in einem Fazit bewertet.

2 Problemstellung

In diesem Kapitel wird die Laborumgebung eingeführt und beschrieben, sowie die damit verbundene Aufgaben-/Problemstellung skizziert.

2.1 Laborumgebung und Versuchsaufbau

Im Labor wird die IT-Landschaft zweier Unternehmen „A“ und „B“ simuliert. Jedes Unternehmen besitzt ein lokales LAN, an denen die pot. Mitarbeiter angeschlossen sind, zudem gibt es mehrere Server mit Hilfe derer verschiedene Dienste angeboten werden sollen. Es folgt eine Liste an Diensten welche Angeboten werden sollen:

- Internetzugang von den Mitarbeiter-Computern.
- Zugang über HTTPS der Webseiten beider Unternehmen.

- Eine Virtuelle Kopplung der beiden Unternehmen mit Hilfe einer sog. Site-to-Site Verbindung.
- Jeder Mitarbeiter der Unternehmen soll die Möglichkeit haben, E-Mails über einen sicheren Mailserver zu verschicken.

Eine weitere wichtige Komponente in dieser IT-Landschaft sind die externen und internen Firewalls, da diese den Grundstein für eine sichere Umgebung legen. In dieser IT-Landschaft gibt es insgesamt 4 Firewalls, jedes Unternehmen hat jeweils eine interne und externe Firewall. Hinter den externen Firewalls beider Unternehmen liegt jeweils die sog. DMZ – Demilitarisierte Zone. In dieser Zone stehen üblicherweise die Unternehmensserver, diese werden nach außen hin von der externen Firewall und nach innen von der internen Firewall geschützt. Jede Firewall läuft auf einem Server, somit besteht die IT-Landschaft insgesamt aus 4 Servern auf welchen die Firewalls laufen, 2 Servern, welche die jeweiligen Unternehmensserver simulieren und einem Server welcher außerhalb der externen Firewall das Internet simulieren soll (vgl. Abb. xxx).

Internetzugang von den Mitarbeiter-Computern. Zugang über HTTPS der Webseiten beider Unternehmen. Eine Virtuelle Kopplung der beiden Unternehmen mit Hilfe einer sog. Site-to-Site Verbindung. Jeder Mitarbeiter der Unternehmen soll die Möglichkeit haben, E-Mails über einen Mailsserver zu verschicken. Eine weitere wichtige Komponente in dieser IT-Landschaft sind die externen und internen Firewalls, da diese den Grundstein für eine sichere Umgebung legen. In dieser IT-Landschaft gibt es insgesamt 4 Firewalls, jedes Unternehmen hat jeweils eine interne und externe Firewall. Hinter den externen Firewalls beider Unternehmen liegt jeweils die sog. DMZ – Demilitarisierte Zone. In dieser Zone stehen üblicherweise die Unternehmensserver, diese werden nach außen hin von der externen Firewall und nach innen von der internen Firewall geschützt. Jede Firewall läuft auf einem Server, somit besteht die IT-Landschaft insgesamt aus 4 Servern auf welchen die Firewalls laufen, 2 Servern, welche die jeweiligen Unternehmensserver simulieren und einem Server welcher außerhalb der externen Firewall das Internet simulieren soll (vgl. Abb. 1).

Jede dieser angesprochenen Komponenten muss entsprechen konfiguriert werden, damit die angesprochenen Dienste fehlerfrei funktionieren können. Technisch gesehen wird jeder dieser Server auf Grundlage einer virtuellen Maschine abgebildet. Jede dieser Maschinen hat Linux als Betriebssystem installiert und vorkonfiguriert, jedoch ohne zusätzliche Pakte, nur die reine Grundinstallation Da die Implementierung und Installation aller dieser Dienste und der damit verbundenen Komponenten den Rahmen dieses Praktikums

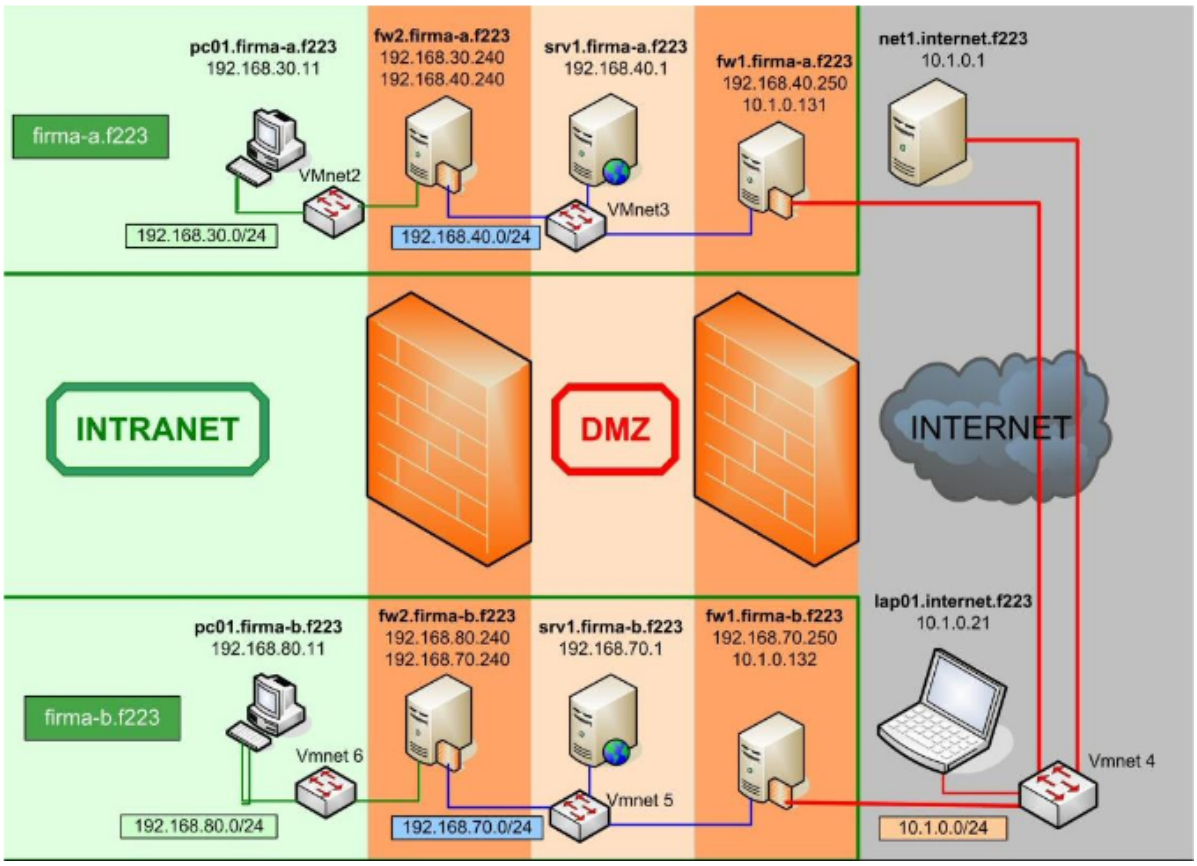

Abbildung 1: Schematischer Aufbau der Laborumgebung im IT-Sicherheitslabor [ND18]

sprengen würde, werden die Aufgabenstellungen zuvor runter gebrochen. Die detaillierte Aufgabenstellung wird im nächsten Abschnitt eingeführt.

2.2 Aufgabenstellung

Wie schon im vorhergehenden Abschnitt beschrieben, gibt es mehrere Dienste, welche in der IT-Landschaft angeboten werden sollen. In diesem Bericht, wird die Virtuelle Kopplung der Unternehmen „A“ und „B“ durch eine „Site-to-Site-“ oder auch „LAN-to-LAN-“ genannt -Verbindung implementiert. Die Problemstellung gilt als gelöst, wenn es möglich ist, dass Unternehmen A eine gesicherte Verbindung zu Unternehmen B aufbauen kann

und die jeweiligen internen Firewalls entsprechend konfiguriert sind. Die Konfiguration der externen Firewalls kann in dieser Aufgabe vernachlässigt werden, hierfür sollen die bereitgestellten internen Firewalls verwendet werden. //TODO Verweis auf Bilder, Begriffe zuordnen.

3 Theoretische Grundlagen

In diesem Kapitel werden die theoretischen Grundlagen eingeführt, welche im Kontext der Aufgabestellung benötigt werden. Dies beschränkt sich auf drei Bereiche, die Netzwerkarchitekturen, Debian GNU Linux 7.11 und IP-Tables. Jede dieser genannten Bereiche wird innerhalb dieses Kapitels eingeführt und in den Aufgabenkontext eingeordnet.

3.1 Netzwerkarchitekturen

Der Bereich Netzwerkarchitekturen ist ein sehr breites Gebiet, deshalb muss dieser zuvor anhand der Anforderungen der Aufgabenstellung abgegrenzt werden.

3.1.1 Die Begriffe Intranet, DMZ und Internet

Das Netzwerk des Labors besteht netzwerktechnisch aus drei Bereichen dem Intranet, der Demilitarisierten Zone und dem Internet. Diese Begriffe werden folgend für den Rahmen dieses Berichts definiert und in den Kontext der Problemstellung eingeordnet.

"Intranet" Nach dem Gabler Wirtschaftslexikon wird ein Intranet als " ein unternehmensinternes Kommunikationsnetz, in dem Daten auf der Basis der Protokollfamilie TCP/IP übertragen werden" definiert. In dieser Arbeit wird der Aspekt der Protokollfamilie "TCP/IP" von vorrangiger Bedeutung sein. Der Punkt des "unternehmensinternen Kommunikationsnetzes", kann für diese Arbeit in den Hintergrund gestellt werden, da sich das Laborpraktikum auf die technischen Umsetzung beschränkt. Ein weiterer wichtiger Aspekt des Intranets ist, dass es nur autorisierten Benutzern gestattet werden soll zuzugreifen.

”Demilitarisierte Zone” Der Begriff demilitarisierte Zone kommt ursprünglich aus dem militärischen Umfeld und beschreibt eine Zone oder Bereich in der sich keine militärischen Streitkräfte gegenüberstehen dürfen, quasi ein neutraler Bereich. In der Netzwerktechnik wird dieser Begriff benutzt, um eine Zone zu beschreiben welche sich zwischen zwei Schutzeinrichtungen befindet. Bei diesen Schutzeinrichtungen handelt es sind meistens um eine externe Firewall und eine interne Firewall. Der Hintergrund für die Einrichtung einer DMZ ist es die Sicherheit der Komponenten und Teilnehmer eines Intranets zu sichern, falls es einen Angriff auf die Komponenten innerhalb der DMZ gibt und diese korumpiert werden sollten. Die Komponenten innerhalb einer DMZ werden als potentielle Opfer oder ”Victims” bezeichnet. Es handelt sich hier meistens um Server welche nach einem Schadensfall einfach durch einen Reboot wiederhergestellt werden können. Als Alternative könnte statt der DMZ ein sog. Application Layer Gateway (APL) eingesetzt werden. Dieser zeichnet sich dadurch, dass er den Netzwerkverkehr komplett auftrennt und sich nach allen Seiten als Kommunikationspartner verhält. Zudem wäre auch eine Lösung aus DMZ und APL[int16]. Im Rahmen des Praktikums wird jedoch lediglich eine DMZ eingesetzt.

”Internet” Das Internet ist ”ein weltumspannendes, heterogenes Computernetzwerk, das auf dem Netzwerkprotokoll TCP/IP basiert. Über das Internet werden zahlreiche Dienste wie z.B. E-Mail, FTP, World Wide Web (WWW) oder IRC angeboten” [Gab]. Ein wichtiger Punkt im Rahmen dieses Praktikums ist, dass das Internet innerhalb der Laborumgebung nur simuliert wird, es besteht also kein richtiger Zugang zum Internet. Dieser Fakt stellt sicher, dass der Versuchsaufbau bei falscher Konfiguration, von außen beschädigt werden könnte. Zudem wird somit sichergestellt, dass bei der Konfiguration der virtuellen Maschinen nur die Versionen der zu Grunde liegenden Images verwendet werden können.

Nachdem die Begriffe Intranet, DMZ und Internet im Kontext der Laborumgebung und Problemstellung definiert und eingrenzt wurden müssen noch weitere Begriffe eingeführt werden. Im folgenden Abschnitt werden die Netzwerkprotokolle oder auch Kommunikationsprotokolle eingeführt, welche im Rahmen des Praktikums verwendet werden.

3.2 Netzwerkprotokolle/Kommunikationsprotokolle

Um eine Netzwerkkommunikation verschiedener Komponenten innerhalb eines Netzwerks zu gewährleisten müssen Netzwerkprotokolle eingesetzt werden.

Im Rahmen des Laborpraktikums werden verschiedene Netzwerkprotokolle eingesetzt, diese lassen sich am besten der entsprechenden Layern im OSI-Schichtenmodell beschrieben. In der nachfolgenden Tabelle werden anhand der Schichten die einzelnen Protokolle eingeordnet, anschließend werden die für dieses Praktikum relevanten Protokolle gesondert beschrieben.

#	OSI-Schicht	Einordnung	Protokolle	Kopplungselemente
7	Anwendungen(Application)	Anwendungs-orientiert	HTTP, FTP, HTTPS, SMTP, DNS, LDAP	Gateway Content-Switch Proxy Layer-4-7-Switch
6	Darstellung(Presentation)			
5	Sitzung(Session)			
4	Transport(Transport)	Transport-orientiert	TCP, UDP, SCTP, SPX	
3	Vermittlung-/Paket(Network)		ICMP, IGMP, IP, IPsec, IPX	RouterLayer-3-Switch
2	Sicherung(Data Link)		Ethernet, Token Ring, FDDI, MAC	BridgeLayer-2-Switch
1	Bitübertragung(Physical)			Netzwerkkabel Repeater Hub

Tabelle 1: OSI-Schichtenmodell

Bevor jedoch die Protokolle eingeführt werden können muss auf den Aufbau eines Datenpaketes geschaut werden.

3.2.1 Datenpakete

In einem Protokoll wird der Aufbau eines Datenpakets definiert, zudem enthält es wichtige Informationen über den Datenaustausch. Es wird definiert, wer der Absender und Empfänger eines Datenpaktes sein soll. Von welchem Typ ein Datenpaket ist, ob es für den Verbindungsaufbau, Verbindungsabbau oder für Nutzdaten genutzt wird. Von größe des Datenpaket, welches beim Empfänger ankommen soll. Wenn es eine mehrteilige Kommunikations ist, muss auch zusätzlich noch die laufende Nummer und die Anzahl der Pakte genau definiert werden. Zuletzt folgt noch eine Prüfsumme, mit Hilfe dieser kann der Empfänger prüfen, ob die Datenpakete auch fehlerfrei angekommen sind.

Alle der Beschriebenen Informationen werden dem ”Header” eines Datenpaktes vorne oder hinten angehängt.

3.3 Debian GNU Linux 7.11

3.4 IP-Tables

3.5 OpenVPN

4 Lösungsskizze

In diesem Kapitel wird sich mit dem Thema befasst, wie sich eine Side-to-Side VPN Verbindung, die die Firmen A und B wie in Kapitel 2.1 beschrieben verbindet. Dazu waren zu Beginn mehrere Vorüberlegungen zu tätigen. Dies sind zum einen, wie wird das innere Netz der Firmen A und B geschützt, dann welcher VPN Dienst kann für diesen Zweck verwendet werden und welche weiteren Strategien braucht es bei der Umsetzung der Security Policies der Firmen.

4.1 Firewall

Wenn eine Firewall aufgebaut werden soll, muss sich zu beginn überlegt werden, welche allgemeine Strategie mit der Firewall gefahren werden soll. Das heißt sollen alle Verbindungen Standardmäßig freigegeben werden und nur explizit nicht erlaubt Verbindungen geblockt werden (Default-Allow-Strategy), oder sollen alle Verbindungen blockiert werden und nur die die explizit erlaubt wurden, geöffnet werden (Default-Deny-Strategy). Im Standardfall wird in Unternehmen, die Strategie Default-Deny verwendet, weshalb sich auch im Versuchsaufbau diese Strategie gewählt wurde. Eine Firewall wird mit Hilfe des Userspace-Programmes IPTABLES (siehe Kapitel 3.4) unter Linux realisiert.

5 Auswertung

6 Fazit

Literatur

[Gab] https://wirtschaftslexikon.gabler.de/definition/internet-37192

[int16] *DMZ, demilitarisierte Zone*. https://www.iternas.com/dmz. Version: 2016, Abruf: 20.07.2018

[ND18] Neuschwander, Jürgen ; Düsterhöft, Sabine: *IT-Sicherheitsarchitekturen Aufgabenstellung zum Praktikum*. March 2018

[Wik] https://de.wikipedia.org/wiki/OSI-Modell#Schicht_4_%E2%80%93_Transportschicht_(Transport_Layer)