Buch Rezension - Manfred Lipp
"VPN - Virtuelle Private Netzwerke - Aufbau und Sicherheit"

Der TecChannel hat mir netterweise das Buch "VPN - Virtuelle Private Netzwerke - Aufbau und Sicherheit" von Manfred Lipp zu einer Rezension überlassen. Dieser Bitte möchte ich mit diesem Blog-Eintrag gerne nachkommen. Ich werde Kapitel-weise durch das Buch gehen und zusammen mit wenigen Sätzen zu dem Inhalt auch eine Einschätzung meiner persönlichen Meinung geben.

Fakten:

Zuerst einmal die nüchternen Fakten:
Titel: "VPN - Virtuelle Private Netzwerke - Aufbau und Sicherheit"
Autor: Manfred Lipp
440 Seiten
Addison-Wesley Verlag
Jahr 2006
ISBN-13: 978-3-8273-2252-4
ISBN-10: 3-8273-2252-4
Preis: 49.95 Euro

Kapitel 1 - Virtuelle Private Netze

Der Autor beschreibt hier die grundlegende Technologie und unterschiedliche Aufbauprinzip. Dazu gehören Verteilung von Aufgaben eines VPN Betreibers (ISP vs. Kunde) wie auch der grundsätzliche Gedanke eines VPNs ein „Netz über ein Netz“ darzustellen.
Das Kapitel motiviert das Thema und gibt gleichzeitig einen Einordnung. Nach der Lektüre dieses Kapitels in der Buchhandlung sollte man wissen, ob die Thematik die gewünschte ist. Viele Referenzen in die folgenden Kapitel geben gleichzeitig einen ausführlichen Überblick des Buchinhalts.

Kapitel 2 – Anforderungen an VPN

Hier werden unterschiedliche Anforderungen, denen ein VPN genügen kann, diskutiert.
Neben Autorisierung und Authentisierung wird die traditionelle Verschlüsselung der Kommunikation ebenso angesprochen, wie auch VPN zu QoS Zwecken einzusetzen. Ebenso kommen Skalierungsaspekte und Setup-Möglichkeiten zur Sprache.
Es wird in ausführlicher Weise dargelegt, wo die Stärken – und damit auch die Schwächen – von VPN Netzwerken sind. Dieses Kapitel sammelt wichtige Aspekte für den Betrieb eines VPNs ohne sich in Details zu verlieren,

Kapitel 3 – Tunneling

Einer der Hauptaspekte des VPN Konzeptes: Wie bekommt man nun die Daten von A nach B? Alle gängigen Protokolle mit ihren unterschiedlichen Layern werden behandelt: IPSec, L2TP. PPTP und MPLS. Ein etwas kurzes Unterkapitel 3.6 Auswahlkriterien hilft bei der Entscheidungsfindung. Letztendlich ist dieses Kapitel nicht sehr ausführlich gehalten, aber im Alltag wird auch nur selten auf dieses Konzept eingegangen, denn es existieren fertige Lösungen, die gegeneinander abgewogen werden wollen. Mit dem Wissen aus diesem Kapitel passiert dieses bzgl. Tunneling problemlos.

Kapitel 4 – Sicherheitstechnologien

Dieses Kapitel ist fokussiert sehr stark auf den algorithmischen Grundlagen der gängigen Kryptographie. Nach einer kleinen Motivation und Einsatz-Beschreibung werden auf anschauliche Weise alle mehr oder weniger aktuellen Algorithmen vorgestellt: Von dem klassischen DES über AES und RC4 zu RSA und Elliptic Curves.
Teilweise fehlen mir als Informatiker etwas die mathematischen Grundlagen, aber das wäre nun auch völlig am Thema des Buches vorbei. So, wie die Prinzipien beschrieben sind, kann man sie begreifen. Man sollte aber bedenken: Dieses Kapitel ist theoretischer Natur! Trotzdem ein wichtiger Aspekt für das Thema VPN.

Kapitel 5 – IP Security (IPSec)

IPSec ist ein weites Gebiet mit vielen Aspekten. Dieses Kapitel schafft es in ca 25 Seiten einen umfassenden Einblick zu geben. Dabei kommen selbst Performancefragen zur Diskussion. Dieses ist beachtlich und wird nur dadurch erreicht, dass keine globale Einordnung und Grundlagen mehr erklärt werden müssen, da diese schon in den vorangehenden Kapiteln behandelt wurden.

Kapitel 6 - IKE Protokoll

IKE adressiert das größte Problem von IPSec: Der Schlüsselaustausch. Dieses Kapitel gibt einen netten Einblick, wenn das Problem selber aber auch in den ersten Kapiteln schon deutlicher gemacht werden dürfen. In diesem Kapitel kommen die existierenden rudimentären Lösungen leider etwas kurz, es wird stattdessen reichlich auf den unterliegenden Prinzipien bis ins kleinste Detail eingegangen. Dafür fehlt aber weder eine abschließende Abschätzung der Performance noch der Sicherheit.

Kapitel 7 – SSL-PN

Es werden Verwendungsmöglichkeiten von SSL dargestellt. Dieses geschieht auf den ersten Seiten unabhängig von VPN – holt sozusagen den Leser bei dem geläufigen HTTP+SSL ab und verallgemeinert. Anschließend wird auf das Thema VPN und SSL eingegangen, wobei netter weise wieder eine Performanceabschätzung das Kapitel abschließt.

Eine gelungene kurze Beschreibung, dieser etwas anderen Thematik, die einige Aspekte von VPN berücksichtigt, andere fallen lässt (Tunneling), wie sie vorher in Kapitel 1 aufgezeigt wurden. Sicherlich erfüllt dieses Setup einige Ansprüche, sodass dieses Kapitel auf jeden Fall lesenswert ist, wenn es auch den klassischen VPN Bereich verläßt.

Kapitel 8 – L2TP / IPSec-Transport

Die wohl häufigste Realisierung von VPNs basiert auf dieser Kombination von Authentisierung-Autorisierung und Tunneling Kombination, weswegen sie auch in diesem Buch nicht fehlen darf. Aufgrund der vorausgehenden Kapitel kann aber auch dieses kurz gehalten werden und beschreibt nur die logische Kombination aus den schon beschriebenen Verfahren.
So einfach kann man es sich als Autor machen, wenn man die richtige Vorarbeit geleistet hat.

Kapitel 9 – Quality of Service in VPN

Dieses Kapitel bezieht sich wohl eher auf die Zukunft als die Gegenwart, wie der Autor auch selber anmerkt werden VPN Technologien heutzutage eher selten oder nur intern zu QoS Zwecken eingesetzt. Dies liegt aber weniger an VPN, sondern eher dadran, dass SLAs (Service Level Agreements) und die daraus resultierenden Verbindlichkeiten noch wenig genutzt werden.
Dieses Kapitel bietet einen netten Ausblick auf Möglichkeiten der VPN Anwendung in der Zukunft, die aber heute schon möglich sind. Damit besonders interessant für Leute, die vielleicht sogar neue Geschäftsfelder erschließen wollen auf in und um das Thema SLA-Realisierung.

Kapitel 10 – Access-Technologien

Hier werden generelle Zugriffsmöglichkeiten auf das Internet oder auch Verbindungstechnologien, die innerhalb von Firmen eingesetzt werden können, beschrieben. Eingangs des Kapitel schreibt der Autor schon, dass kein direkter Zusammenhang zu VPN besteht, so ist dieses Kapitel mit ca 20 Seiten auch eher knapp gehalten.
Auch wenn die kurzen Beschreibungen gut und prägnant sind – dieses Thema gehört meiner Meinung nach nicht wirklich in das Buch – es eröffnet ein großes Thema ohne hierüber auf den wenigen Seiten einen kompletten Überblick liefern zu können.

Kapitel 11 – Design und Realisierung

Der Autor führt zum Abschluss des Buches die theoretischen und Protokoll-lastigen Kapitel zusammen indem er eine allgemeine Beschreibung zur Realisierung eines VPN Netzwerkes gibt. Das Wort „Realisierung“ in der Überschrift mag aber verwirren. Es geht eher um den Entwicklungs-Prozess und die Etablierung eines VPNs im Firmen Umfeld und damit auch betriebswirtschaftliche Dinge wie die Anschaffung von Hardware als um eine Realisierung eines VPNs im Administrations-Sinne.
Direkt angebunden an die vorhergehenden Kapitel ist dieser Abschnitt nicht, trotzdem überrascht

das Buch positiv durch solch eine Praxis-nahe Betrachtung der Thematik.

Fazit:

Ein Buch, wie es perfekt (für mich) ist. Es vermittelt sowohl die nötigen theoretischen algorithmischen Grundlagen, wie auch die genutzten Technologien und Philosophien neben einem Einstieg in die (praxisnahe) Realisierungen. Dieses Buch stellt aber keine Betriebs und oder Aufbau-Anleitung für ein VPN Netzwerk im Sinne einer Netzwerk-Administration dar. Es sollte zur Einarbeitung dienen und Hintergrund wissen vermitteln. Das ggf. nötige Detailwissen von Implementierungen kann nach der Lektüre ohne Probleme von Webseiten erworben werden, da man mit den nötigen Begriffe vertraut ist.
Das heißt: Gewohnt hohe Addison-Wesley Qualität zu einem fairen Preis von knapp 50 Euro.

Wie es im IT Bereich nun mal sein muss, ist Papier abgestaubt, wenn es aus der Druckmaschine kommt. So werden aktuellste Trends dieser Monate, wie IKEv2, leider nicht abgehandelt. Der – in meinen Augen – sehr viel versprechende Ansatz MobIKE wird immerhin kurz erwähnt. Gerade solche Bücher verlieren hierdurch aber nur wenig an ihrem Wert, denn die Grundlagen bleiben zum größten Teil erhalten. Eine ideale Voraussetzung um bei Gelegenheit eine 2. Auflage raus zubringen, auf die sich zu warten aber nicht lohnt!
Insgesamt: Daumen hoch!

zu meiner Person:

Da ich in auf dieser Webseite bisher nicht in Erscheinung getreten bin, möchte ich mich ganz kurz vorstellen. Mein Name ist Henning Mersch, ich habe 2003 mein Diplom Informatik mit 2. Hauptfach Biologie an der Uni Bielefeld bekommen. Zwischenzeitlich habe ich am Forschungszentrum Jülich im Bereich Grid Computing gearbeitet und promoviere zur Zeit an der RWTH Aachen am Lehrstuhl für Prozessleittechnik. Meine Tätigkeiten im Administrations-Bereich begleiten meine wissenschaftliche Arbeit von Zeiten als studentische Hilfskraft und wissenschaftlicher Mitarbeiter in Bielefeld (www.bibiserv.de) an bis heute. VPN selber spielte dabei allerdings nur im privaten Bereich eine Rolle. Weitere Informationen und Interessen, wie auch Kontaktaufnahme gerne über meine Homepage: www.henning-mersch.de