Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

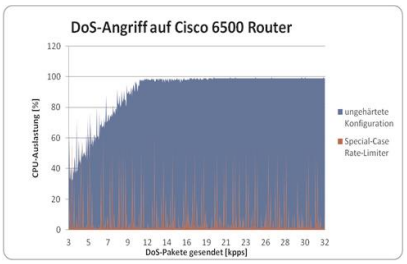
InIT Institut für angewandte
Informationstechnologie

Hardening einer DMZ-Infrastruktur gegen DDoS-Attacken

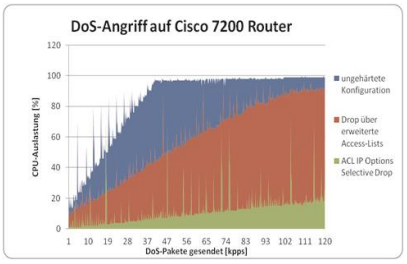
Denial of Service (DoS)-Attacken haben meist zum Ziel, die über das Internet verfügbaren Dienste einer Organisation oder eines Unternehmens funktionsunfähig zu machen. Der Schaden, der dabei entsteht, ist nicht bloss wirtschaftlicher Natur, sondern beeinflusst das Image des Opfers oft negativ. Entsprechend umfangreich sind die Massnahmen, die Unternehmen ergreifen, um sich gegen solche Angriffe zu schützen. Deren Internet Access Router spielen als direkte Schnittstelle zum Internet Service Provider eine wichtige Rolle. Durch eine Absicherung dieser Geräte gegen DoS-Angriffe (Härtung) ist es möglich, sowohl die Geräte selbst, als auch den Rest der Infrastruktur resistenter gegen jene Attacken zu machen. In dieser Diplomarbeit ging es darum, die zwei in einem Finanzinstitut weltweit eingesetzten Internet-Access-Routertypen Cisco 6500 und Cisco 7200 gegen einen spezifischen DoS-Angriff mit Paketen mit gesetzten IP-Options (optionales Feld im IP-Header) zu härten und sicherzustellen, dass dabei der legitime Datenverkehr in keiner Weise beeinträchtigt wird.
Auf Basis einer umfassenden Analyse der produktiven DMZ-Infrastruktur des Finanzinstitutes wurde für dieses ein Massnahmenkatalog erstellt. Die Umsetzung der favorisierten Vorschläge erfolgte in der dafür im Rahmen der Diplomarbeit aufgebauten Testumgebung. Letztendlich wurde pro Routertyp die jeweils beste Härtungsmassnahme mit einer Aufwandsabschätzung für deren Umsetzung und dem weiteren Vorgehen vorgeschlagen.
Das Resultat dieser Diplomarbeit ist eine Empfehlung mit folgendem Ergebnis: Der Routertyp Cisco 6500 kann durch so genannte Special-Case Rate-Limiter effektiv gegen ein Flooding von Paketen mit gesetzten IP-Options geschützt werden. Dabei wird nur ein kleiner Teil der gefährlichen Pakete verarbeitet, der Rest wird, ohne den Prozessor zu beanspruchen, verworfen. Der legitime Datenverkehr ist von dieser Härtungsmassnahme in keiner Weise betroffen. Für den Routertyp Cisco 7200 wird hingegen mit Vorbehalt vorgeschlagen, eine Härtung über "ACL IP Options Selective Drop" zu realisieren. Dabei werden alle Pakete mit IP-Options verworfen. Der Fall "IP-Options" gilt in dieser Arbeit lediglich als Proof-of-Concept. Weiterführende Vorschläge betreffen Spezialfälle, die eine ebenso hohe Gefahr für die Router bergen.

Diplomierende
Manuel Erni
Stefan Manuel Meier

Dozent
Marc Rennhard



Die Prozessorauslastung des gehärteten Cisco 6500 Routers bleibt bei steigender DoS-Paketrate konstant tief (rot). DoS-Pakete werden verworfen, bevor sie die CPU in Anspruch nehmen. Als Folge zeigen (D)DoS-Attacken mit IP-Options keine Wirkung.



Im Falle eines Flooding-Angriffes mit Paketen mit IP-Options führt die Härtung des Cisco 7200 Routers mittels "ACL IP Options Selective Drop" zu einer Verminderung der CPU-Auslastung um Faktor achtzehn gegenüber dem ungehärtetem Zustand.