HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

ELEKTROTECHNIK

Studiengang	**Elektrotechnik**
Diplomandin / Diplomand	**Dave Marbacher und Marcel Rölli**
Diplomjahr	**2002**
Titel der Diplomarbeit	**ISP Performance- und Security- Tests**
Examinatorin / Examinator	**Prof. Dr. Peter Heinzmann**
Industriepartner	**Checkpoint/cnlab AG**

Kurzfassung der Diplomarbeit

Um sich in die Thematik von Security- und Performance Parametern in Netzwerken einzuarbeiten, war es in einem ersten Schritt notwendig, die Funktionsweise von Intrusion-Detection Systemen (IDS) kennen zu lernen. Als IDS wurde das frei verfügbare Snort verwendet, welches in der Lage ist, auffällige Verhaltensweisen in einem Netzwerk zu detektieren und auszuwerten.

Parallel dazu wurde eine Analyse und ein Review für den bestehenden Providertest durchgeführt. Dieses Programm erlaubt es, Aussagen über die Leistungsfähigkeit von ISPs zu machen und diese miteinander zu vergleichen. Um den Providertest auf Linux zu portieren, war es notwenig, sich in dieses Betriebssystem ein zuarbeiten. Dazu wurde die Distribution Linux-Mandrake 9.0 verwendet.

Der Providertest wurde unter anderem um eine Datenbank-Anbindung (mysql) und einem automatischen Upload sämtlicher Messdaten in eine zentrale Auswertungsstelle erweitert. Unter diesen Messdaten befinden sich auch diejenigen Attacken, welche durch Snort detektiert wurden.

Neben Snort wurden auch Security-Gateways (S-Boxen) für die Beurteilung der „Sicherheit“ von ISP eingesetzt. Die S-Boxen sind mit einer hardwaremässigen Firewall ausgerüstet. Das nötige Fachwissen für den Umgang mit den S-Boxen musste gelernt werden. Um die Logs der Firewall zentral zu erfassen, wurde es notwendig, einen Management-Server der Firma Check Point auf zusetzten.

Generell konnte festgestellt werden, dass die meisten Attacken in einem Netzwerk (ca. 85%) auf den Port 137 (netbios), gefolgt von Port 80 (http) ausgeübt werden. Auf dem Netz des ISP **bluewin** werden momentan die meisten Attacken detektiert. Ausgangspunkt der meisten Angriffe werden von einem Topleveldomain .net unternommen.