HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Studienarbeit

Abteilung	**I**
Name der Studenten	**Bösch Christoph** **Rölli Adrian**
Diplomjahr	**2003**
Titel der Studienarbeit	**ISP Security Map**
Examinator	**Prof. Dr. P. Heinzmann**

Kurzfassung der Studienarbeit

Möchte man verschiedene ISPs auf Unterschiede im Bezug auf Sicherheit unterscheiden, müssen zuerst Daten gesammelt werden. Dies geschieht mittels zwei Arten von Messsonden:

- SBox: Die SBox von Sofaware ist ein „Security Gateway“ und besitzt eine integrierte Firewall. Um deren Logs zentral sammeln zu können, wurde ein Management-Server der Firma Checkpoint installiert.
- Snort: Snort ist ein Open Source IDS (Intrusion Detection System). Die bisherigen Performance-Sonden, welche unter Windows laufen, können nun um Snort erweitert werden. Wegen Stabilitätsproblemen wird es aber mittels VMWare unter Linux eingesetzt.

In einem Testnetz der Swisscom wurde eine vollständige Messumgebung aufgebaut, und an diversen anderen Orten wurden Teile davon in Betrieb genommen.

Die so gesammelten Logdaten werden mit einem Java-Programm an eine zentrale Datenbank bei der Firma cnlab AG geschickt (über ein JSP-Webinterface). Ebenso werden sie an Dshield.org übermittelt.

Für die Auswertung der Daten wurden einige grundlegende Darstellungskonzepte erarbeitet und für die bestehende cnlab-Plattform (Tomcat, JSP, JCharts) implementiert. Allerdings konnte eine Detektion für Attackenmuster, wie sie z.B. von Scanning-Tools generiert werden, nicht umgesetzt werden, da dies den Rahmen dieser Arbeit gesprengt hätte.

Die Firma Swisscom hat bei dieser Arbeit als Industriepartner mitgemacht, da sie für ihre Kunden mit sicherem Internetanschluss (SecurePoP, Schulen ans Internet) eine ähnliche Lösung in Betracht zieht.