HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Studienarbeit

Abteilung	**Informatik**
Name der Diplomandin / des Diplomanden	**Andreas Rüst** **Oliver Würmli**
Diplomjahr	**2003**
Titel der Diplomarbeit	**OPSEC und IDS-Firewall Kopplung**
Examinatorin / Examinator	**P.Heinzmann**

Kurzfassung der Diplomarbeit

Ausgangslage: Der Verbesserung der Internet-Sicherheit wurde in der letzten Zeit vermehrt Aufmerksamkeit geschenkt. Es geht nicht mehr nur darum einzelne Sicherheitssysteme, wie z.B. Firewalls zu installieren, sondern ein geordnetes Zusammenspiel zwischen diesen zu gewährleisten. Die Möglichkeit zur Integration von verschiedenen Sicherheitssystemen bietet die Firma Checkpoint mit ihrer Open Plattform for Security (OPSEC). Anbieter von Security - Systemen sind heute fast gezwungen OPSEC Kompatibilität anzubieten, da es heute der Quasi Standart ist.

Ziel: Die Kopplung eines Intrusion Detection System (IDS) mit einem Firewall (FW) war das Ziel dieser Studienarbeit. Dazu sollten die notwendigen Kenntnisse auf den Gebieten IDS und FW erworben werden und jeweils ein Produkt auch in Betrieb genommen werden. Da die Kopplung über OPSEC erfolgt, mussten auch hier die notwendigen Kenntnisse erarbeitet werden.

Ergebnis: Nach der Einarbeitung in die Gebiete IDS und FW haben wir uns entschieden das Open Source IDS Snort und der FW1 von Checkpoint einzusetzen. Neben den Technologiestudien zu diesen Gebieten, haben wir zwei Labs geschrieben, die in der Vorlesung Netzwerksicherheit eingesetzt werden können.
Für Snort haben wir ein PlugIn geschrieben, welches den Firewall umkonfiguriert, falls ein Angriff erfolgt und detektiert wird.

Fazit: Die Inbetriebnahme, Konfiguration und Betrieb von Sicherheitssystem ist mit einigen Stolpersteinen verbunden., so kann bei Konfigurationsfehlern das ganze Sicherheitssystem nutzlos sein.
Das OPSEC API ist sehr umfangreich und es braucht eine gute Einarbeitung, um OPSEC richtig zu verstehen und anwenden zu können. Richtig angewandt ist sie jedoch sehr mächtig.