HOCHSCHULE
RAPPERSWIL
HSR

Kurzfassung der Diplomarbeit

Abteilung	**Informatik**
Name der Diplomandin / des Diplomanden	**Peter Yoichiro Bühler** **Thomas Zollinger**
Diplomjahr	**2000**
Titel der Diplomarbeit	**Network-based Intrusion Detection System / Experimental Engine**
Examinatorin / Examinator	**Walter Sprenger, CSNC AG , Ivan Bütler, CSNC AG**

Kurzfassung der Diplomarbeit

Intrusion Detection Systeme (IDS) dienen dazu, Angriffe von Mitarbeiter und Hacker auf ein Computersystem zu detektieren. Das Ziel dieser Diplomarbeit war die Entwicklung einer experimentellen Engine eines Intrusion Detection Systems.

In einem ersten Schritt wurde eine Bedrohungsanalyse erstellt. Sie zeigt auf, wo sich die Angriffspunkte in einem Computernetzwerk befinden, wer die Personen sind und welche Ziele sie verfolgen. Es stellte sich heraus, dass von einem Mitarbeiter mit böswilligen Absichten, die grösste Gefahr ausgeht. Dies ist der Fall, weil diese Tätergruppe Zugriff auf die verschiedenen Systeme hat.

Danach wurde eine Analyse getätigt, wie man die Integrität eines Detektionsprogramms sicherstellen kann. Das Resultat war, dass sich Software nicht oder nur ungenügend durch Software schützen lässt.

Im dritten Schritt wurde die Experimental Engine erstellt. Sie besteht aus zwei verschiedenen Programmen: Einem Agent und einer Management Konsole.

Mit der Management Konsole können die verschiedenen Agenten zentral verwaltet und konfiguriert werden. Sie wurde komplett in Java geschrieben und läuft daher auf jedem Computer mit einer Java Virtual Machine. Die Management Konsole empfängt alle Meldungen und Alarme von den Agenten.

Der Agent wird auf jedem Computer mit Windows NT 4.0, der überwacht werden soll, installiert. In ihm befinden sich zwei verschiedene Detektionsprogramme. Das IDS Snort 1.6.3, welches als Open-Source verfügbar ist, und ein Event-Viewer.

Snort wurde für diese Diplomarbeit angepasst und deshalb sind einige Routinen abgeändert. Tritt eine Intrusion auf, so wird sofort eine Meldung an die Management Konsole gesendet.

Der Event-Viewer wartet auf neue Einträge ins Event-Log und meldet diese der Management Konsole.

Alle aufgetretenen Meldungen und Alarme werden lokal beim Agenten in einem Log-File gespeichert und an die gleichzeitig an die Management Konsole gesandt. Falls keine Verbindung zur Management Konsole besteht werden alle Meldungen und Alarme zusätzlich in einem verschlüsselten Security-Log gespeichert. Diese Einträge werden nach erfolgter Verbindung an die Management Konsole gesandt.

Damit keine Meldungen oder Alarme während der Übertragung verändert werden können, wird die Kommunikation zwischen der Management Konsole und den Agenten ist mit SSL 3.0 verschlüsselt.

HOCHSCHULE
RAPPERSWIL
HSR