Fachhochschule Nordakademie Elmshorn

Diplomarbeit - Zusammenfassung

zur Erlangung des akademischen Grades
Diplom-Wirtschaftsinformatiker (FH)

Steigerung der Netzwerksicherheit durch „Network Behavior Anomaly Detection“: Eine Analyse unter technischen und wirtschaftlichen Gesichtpunkten

Fachbereich:	Informatik
Verfasser:	Christian Göttsche (Ma.Nr. 2053)
	cg@christian-goettsche.de
Betreuer:	Dipl.-Inf. Uwe Neuhaus
Co-Betreuer:	Dipl.-Inf. Helmut Guttenberg
Betrieblicher Betreuer:	Dipl.-Ing. Thorsten Trapp

Diplomarbeit: 9. Januar 2007
Zusammenfassung: 5. November 2007

Diplomarbeit - Zusammenfassung

Die Diplomarbeit beschäftigt sich mit dem Thema: *„Steigerung der Netzwerksicherheit durch "Network Behavior Anomaly Detection": Eine Analyse unter technischen und wirtschaftlichen Gesichtspunkten*". Die Sicherheit von Netzwerken wird weitestgehend durch ein Regelwerk gewährleistet. Komplexe Infrastrukturen setzen hierbei ebenso komplexe Regelwerke voraus. Dabei bleibt das Restrisiko eines unvollständigen Regelwerks ständig bestehen. Ebenso bleibt die Frage offen, ob jedes erdenkbares Sicherheitsrisiko durch das Regelwerk abgedeckt ist. Wird hingegen der *gewünschte* Datenverkehr im gesamten Netzwerk abstrakt als *Normalzustand* definiert, ist es die Aufgabe der *Network Behavior Anomaly Detection (NBAD)*[1] jegliche Abweichungen zu erkennen und zu melden.

In dieser Arbeit wird einleitend der Begriff der Sicherheit festgelegt. Auf dieser Grundlage werden die verschiedenen klassischen Sicherheitssysteme der *Prävention* und *Detektion* vorgestellt und in ihrer Funktionsweise erläutert. Es erfolgt eine Klassifizierung von *NBAD* vor dem Hintergrund klassischer Sicherheitssysteme und eine Vorstellung der Funktionsweise.

- **Präventive Sicherheitssysteme**
  Firewall-Konzepte, Anti-Viren-Lösungen

- **Detektive Sicherheitssysteme**
  Intrusion Detection Systeme

- **Anomaly Detection**
  Funktionsumfang von NBAD

Um eine Untersuchung der Netzwerksicherheit durchzuführen wird eine mögliche Netzwerkstruktur eines Unternehmens definiert. Das Testnetzwerk setzt sich hierbei aus mehreren Teilen zusammen. Es wird ein Unternehmen definiert mit einer Hauptverwaltung, drei angebundenen Außenstellen in verschiedenen Ländern und mehreren Außendienstmitarbeitern. Das Sicherheitskonzept ist gemäß den Empfehlungen des *Bundesamtes für Sicherheit in der Inforationstechnik (BSI)* aufgebaut.

- **Betrachtungsumfeld**
  Testnetzwerk mit BSI-konformer Netzwerksicherheit

- **Datensammlung**
  Konzept für die Erfassung der Daten-Flows im gesamten Testnetzwerk (sFlow)

Die Untersuchung der gesteigerten Netzwerksicherheit erfolgt, indem die Gefahrenpotentiale mit und ohne den Einsatz von *NBAD* analysiert werden. Hierzu wird eine Auswahl über 15 relevante Sicherheitsvorfälle sowie deren Gefahrenpotentiale getroffen.

- **Auswahl der Angriffszenarien**
  Relevante Angriffe: Deren Ziele und Auswirkungen

- **Untersuchung der Netzwerksicherheit**
  Gefahrenpotential mit und ohne Unterstützung durch NBAD

In der anschließenden Auswertung erfolgt einer Sicherheitsbewertung um hieraus den Sicherheitszuwachs ermitteln zu können. Dabei werden die Unsicherheiten durch eine unvollständige *Daten-Flow*-Erfassung berücksichtigt. Weiterhin wird das bestehende Restrisiko erläutert sowie die Frage untersucht, ob *NBAD* präventive Sicherheitsmaßnahmen ersetzen kann.

Um die Wirtschaftlichkeit einer *NBAD-Lösung* nachzuweisen werden die potentiellen Schäden der Angriffszenarien, sowie deren Eintrittswahrscheinlichkeit ermittelt. Diese Schäden werden den Kosten einer Implementierung und dem Betrieb einer *NBAD-Lösung* gegenüber gestellt. Hierzu wird der *Return on Security Investment (RoSI)* vorgestellt. Auf dieser Grundlage erfolgt die Bewertung einer *NBAD-Lösung*.

- **Wirtschaftlichkeitsanalyse**
  Potentielle wirtschaftliche Schäden

- **Investitionsbewertung**
  RoSI einer NBAD-Lösung

[1] Eine weitere gängige Bezeichnung ist *Network Behavior Analysis (NBA)*