

**Denis Aumüller**

Vergleich einer kommerziellen Intrusion  
Detection Software mit einer  
OpenSource-Lösung im Bezug aus Leistung,  
Anwendbarkeit und Kosten

**Diplomarbeit**

## **Bibliografische Information der Deutschen Nationalbibliothek:**

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2003 Diplomica Verlag GmbH  
ISBN: 9783832468538

**Denis Aumüller**

**Vergleich einer kommerziellen Intrusion Detection Software mit einer OpenSource-Lösung im Bezug aus Leistung, Anwendbarkeit und Kosten**



---

Denis Aumüller

# **Vergleich einer kommerziellen Intrusion Detection Software mit einer OpenSource-Lösung im Bezug aus Leistung, Anwendbarkeit und Kosten**

**Diplomarbeit  
an der Fachhochschule Worms  
Fachbereich Informatik  
3 Monate Bearbeitungsdauer  
Mai 2003 Abgabe**



***Diplom.de***

Diplomica GmbH \_\_\_\_\_  
Hermannstal 119k \_\_\_\_\_  
22119 Hamburg \_\_\_\_\_

Fon: 040 / 655 99 20 \_\_\_\_\_  
Fax: 040 / 655 99 222 \_\_\_\_\_

agentur@diplom.de \_\_\_\_\_  
www.diplom.de \_\_\_\_\_

ID 6853

Aumüller, Denis: Vergleich einer kommerziellen Intrusion Detection Software mit einer OpenSource-Lösung im Bezug auf Leistung, Anwendbarkeit und Kosten  
Hamburg: Diplomatica GmbH, 2003  
Zugl.: Worms, Fachhochschule, Diplomarbeit, 2003

---

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomatica GmbH, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Diplomatica GmbH  
<http://www.diplom.de>, Hamburg 2003  
Printed in Germany

---

# Inhaltsverzeichnis

<b>Vergleich einer kommerziellen Intrusion Detection Software mit einer OpenSource-Lösung im Bezug auf Leistung, Anwendbarkeit und Kosten.....</b>	<b>1</b>
<b>1. Einleitung.....</b>	<b>4</b>
1.1 Aufgabenstellung.....	4
1.2 Eidesstattliche Erklärung.....	4
<b>2. Einführung in das Thema IDS.....</b>	<b>5</b>
2.1 Definition „Intrusion Detection“ .....	5
2.2 Was ist ein „Intrusion Detection System“ (IDS) ? .....	5
2.3 Wieso IDS einsetzen? .....	6
2.4 Arten von IDS.....	7
2.5 Erkennung von Angriffsmustern .....	10
2.6 Einsatz in einem geschwichten Netzwerk.....	13
<b>3. Produktvorstellung .....</b>	<b>16</b>
3.1 Einleitung .....	16
3.2 Produkt Matrix.....	16
3.3 Kurzvorstellung der Produkte.....	18
<b>4. Vergleich der Softwarelösungen.....</b>	<b>20</b>
4.1 „Prelude 0.8.1“ .....	20
4.2 „RealSecure 6.7“ .....	32

---

<b>5. IDS in der Praxis</b> .....	<b>44</b>
5.1 Einleitung .....	44
5.2 Entwicklung der Angriffskomplexität.....	45
5.3 Einige der bekanntesten Angriffe.....	46
5.4 Testreihe mit Angriffen .....	47
5.5 Realisierung einer eigenen Signatur.....	55
5.6 Warnmeldungen .....	61
5.7 Reaktionen bei erkanntem Angriff.....	62
5.8 Tests im Internet.....	63
<b>6. Kosten-Nutzen-Betrachtung</b> .....	<b>68</b>
6.1 Dokumentation .....	68
6.2 Installation .....	69
6.3 Konfiguration .....	70
6.4 Managebarkeit.....	71
6.5 Integration in die bestehende IT-Infrastruktur .....	71
6.6 Performance und Skalierbarkeit .....	71
6.7 Stabilität.....	72
6.8 Preis / Leistung.....	73
<b>7. Fazit und Ausblick</b> .....	<b>74</b>
7.1 Zusammenfassung .....	74
7.2 Ausblick.....	76
7.3 Fazit.....	77
<b>8. Anhang</b> .....	<b>78</b>
8.1 Abkürzungen .....	78
8.2 Verwendete Programme .....	79
8.3 Literatur-Verzeichnis.....	79
8.4 Wichtige Links .....	80
8.5 Newsgroups .....	80
8.6 Danksagung .....	80

---

# 1. Einleitung

## 1.1 Aufgabenstellung

Das Ziel im Rahmen dieser Diplomarbeit für die Firma BASF IT Services B.V. ist es einen Vergleich zwischen der vorhandenen kommerziellen Intrusion Detection Software „RealSecure“ und einer kostenlosen OpenSource-Lösung namens „Prelude“ anzustellen.

Dieser Vergleich soll sowohl die Features, als auch Integration, Kosten und Nutzen berücksichtigen, da die BASF IT Services B.V. im Rahmen ihres Managed Security Konzeptes ihren Kunden maßgeschneiderte und kostengünstige IDS Produkte anbieten möchte.

## 1.2 Eidesstattliche Erklärung

Hiermit erkläre ich an Eides Statt, dass ich die vorliegende Diplomarbeit selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel während meines 8. Semesters im Zeitraum vom 2. März 2003 bis zum 31. Mai 2003 bei der Firma BASF IT Services B.V erstellt habe. Alle Ausführungen, die wörtlich oder sinngemäß übernommen wurden, sind als solche gekennzeichnet. Die Diplomarbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Ludwigshafen, den 31.05.2003



.....  
Denis Aumüller