1. Einleitung S. 6
- 1.1 Einführung in die Thematik S. 7
- 1.2 Terminologie S. 9
  - 1.2.1 Definitionen S. 9
  - 1.2.2 Klassifikation von Malware S. 13
  - 1.2.3 Klassifikationen von Viren S. 13
    - 1.2.3.1 Klassifikation nach Plattform S. 14
    - 1.2.3.2 Klassifikation nach Verbreitung S. 16
- 1.3 Das Virus Test Center der Universität Hamburg S. 16

2. Qualitätskriterien für die Erkennung von bösartiger Software S. 18
- 2.1 Allgemeine Qualitätsanforderungen an Software S. 18
- 2.2 Quantitative Kriterien für die Erkennung von bösartiger Software S. 20
  - 2.2.1 Erkennungsrate S. 20
  - 2.2.2 Erkennungsgenauigkeit und -zuverlässigkeit S. 21
  - 2.2.3 Häufigkeit von Falschmeldungen S. 22
  - 2.2.4 Unterstützung von Dateiformaten S. 23
  - 2.2.5 Geschwindigkeit S. 24
  - 2.2.6 Reparatur von infizierten Dateien S. 24
  - 2.2.7 Beispiele S. 24
- 2.3 Qualitative Kriterien für die Erkennung von bösartiger Software S. 27
  - 2.3.1 Bedienbarkeit und Benutzerfreundlichkeit S. 28
  - 2.3.2 Stabilität S. 28
  - 2.3.3 Funktionalität S. 28
  - 2.3.4 Korrektheit S. 29
  - 2.3.5 Anpaßbarkeit und Wartungsfreundlichkeit S. 29
  - 2.3.6 Administrierbarkeit und -aufwand S. 30
  - 2.3.7 Beispiel S. 30
- 2.4 Andere Kriterien S. 31

3. Qualitätsrichtlinien und Methoden zur Bestimmung der Erkennungsgüte von Anti-Malware-Software S. 33
- 3.1 Testen von Software S. 33
- 3.2 Qualitätsrichtlinien für das Testen von Anti-Malware Software S. 34
  - 3.2.1 Vollständigkeit und Größe der Testmenge S. 35
  - 3.2.2 Qualität der Testmenge S. 38
  - 3.2.3 Nachvollziehbarkeit der Ergebnisse S. 38
  - 3.2.4 Objektivität und Herstellerunabhängigkeit S. 39
  - 3.2.5 Aussagekraft und Nützlichkeit der Ergebnisse S. 39
- 3.3 Methoden für die Messung von quantitativen Kriterien S. 40
  - 3.3.1 Messung von quantitativen Qualitätskriterien S. 42
  - 3.3.2 Testen der Erkennung im On-demand Modus S. 43
  - 3.3.3 Testen der Erkennung im On-access Modus S. 44
- 3.4 Methoden für die Qualitätsbestimmung von qualitativen Kriterien S. 46

4. Die Methodik und das Verfahren des VTC S. 49
- 4.1 Grundlagen und Allgemeines zum Virus Test Center S. 49
  - 4.1.1 Grundsätze des VTC und Ziele der Tests S. 50
  - 4.1.2 Getestete Kriterien S. 51
  - 4.1.3 Testumgebung S. 52
  - 4.1.4 Testmenge S. 53
- 4.2 Die Testmethotik S. 56
  - 4.2.1 Überblick über die Testmethodik S. 57
  - 4.2.2 Beschreibung der Aufgaben und Arbeitsschritte S. 58
    - 4.2.2.1 Virenkollektionen zusammentragen S. 58
    - 4.2.2.2 Viren sortieren S. 60
    - 4.2.2.3 Testprodukte anfordern S. 61
    - 4.2.2.4 Testen S. 62
    - 4.2.2.5 Auswerten S. 67
    - 4.2.2.6 Endauswertung S. 69
    - 4.2.2.7 Testbericht erstellen S. 69
    - 4.2.2.8 Testbericht veröffentlichen S. 74
  - 4.2.3 Aufgabenverteilung S. 75
  - 4.2.4 Sicherstellung der Qualität S. 76
- 4.3 Durchgeführte Anti-Malware-Tests S. 79
  - 4.3.1 Periodische Tests der Erkennung S. 79
  - 4.3.2 Antivirus Repairtest (ART-Test) S. 80
  - 4.3.3 Heureka Test S. 81
  - 4.3.4 Überblick über durchgeführte Tests S. 82

5. Andere Tests von Anti-Malware-Software S. 86
- 5.1 AV-Test.de S. 86
- 5.2 ICSA-Labs S. 87
- 5.3 West Coast Labs S. 88
- 5.4 Virus Bulletin S. 89
- 5.5 Tests von Antivirenprodukten in Computerzeitschriften S. 89
- 5.6 Vergleich anderer Anti-Malware Tests mit dem VTC Test S. 90

6. Erweiterungen und Verbesserungen für das Testverfahren des VTC S. 93
- 6.1 Probleme und Schwächen des VTC-Verfahrens S. 93
  - 6.1.1 Kapazitätsprobleme S. 93
  - 6.1.2 Organisatorische Probleme S. 95
  - 6.1.3 Schwächen des VTC-Verfahrens S. 96
- 6.2 Die Datenbank VTED und erweiterte Möglichkeiten der Ergebnisanalyse S. 98
  - 6.2.1 Vorteile einer Datenbank zur Ergebnisanalyse S. 98
  - 6.2.2 Der Aufbau der Datenbank VTED S. 99
  - 6.2.3 Der Datenimport S. 101
- 6.3 Grafische Darstellung der Ergebnisse S. 103
- 6.4 Untersuchung der langfristigen Entwicklung der Erkennung S. 106

6.5 Automatische Bewertung der Ergebnisse S. 108
6.6 Automatische Erstellung des Testberichtes S. 111

7. Betrachtung von aufbereiteten Testergebnissen am Beispiel aktueller VTC-Tests S. 115
7.1 Grafiken zum Test 2002-03 (Heureka II) S. 115
7.2 Grafiken und Analysen zum Test 2001-10 S. 122
7.2.1 Windows32-Abweichungen der Erkennungsrate S. 122
7.2.2 Ergebnisgrafiken S. 124
7.3 Betrachtungen und Grafiken von Testergebnissen mehrerer Tests S. 131
7.3.1 Tabellen von Zeitreihen S. 131
7.3.2 Grafiken von Zeitreihen S. 134

8. Zusammenfassung und Ausblick S. 137

Abbildungsverzeichnis S. 139
Tabellenverzeichnis S. 141
Literaturverzeichnis S. 142

Danksagung S. 148

Anhang A - Zusätzliche und genaue Angaben zum Verfahren des Virus Test Centers A-1 bis A-16
Anhang B - Benutzung, Wartung und ausgewählter Quellcode der Datenbank VTED B-1 bis B-12
Anhang C - Zeitreihen der Erkennungsrate C-1 bis C-8