8. Zusammenfassung und Ausblick

In dieser Arbeit ist gezeigt worden, wie man die - durch Anti-Malware-Programme gewährleistete - Qualität der Erkennung von bösartiger Software bestimmen kann. Als Grundlage dazu wurden in Kapitel 2 Qualitätsmerkmale für Anti-Malware-Software und in Kapitel 3 Anforderungen an einen Test zur Bestimmung dieser Qualität untersucht. In Kapitel 4 wurde die Methodik des Virus Test Centers beschrieben und so ein ausgereiftes Verfahren zur Bestimmung der Qualität von Anti-Malware-Programmen ausführlich dargestellt. Dieses Verfahren wurde in Kapitel 5 mit anderen Testinstitutionen von Anti-Malware-Software verglichen.

Es wurde deutlich, daß nur ein Test mit einer großen Testmenge an Musterdateien aussagekräftige Testergebnisse über die Qualität von Anti-Malware-Software liefert. Um aber Protokolldateien von Scanprozessen auf großen Testmengen auswerten zu können, sind automatisierte Verfahren nötig. Nur durch Automation des Testverfahrens wird die Durchführung eines Testes mit einer Vielzahl von Testprodukten auf großen Datenmengen an Musterdateien möglich.

In der vorliegenden Arbeit wurden in diesem Zusammenhang datenbankbasierte Verfahren zur automatischen Erstellung, Bewertung und Veröffentlichung von Testergebnissen der Qualitätsbestimmung der Erkennung von bösartiger Software vorgestellt. Die durchgeführten Erweiterungen des VTC-Verfahrens werden mit Hilfe der im Rahmen dieser Arbeit weiterentwickelten relationalen Datenbank *VTED* realisiert. Durch den Import von Testergebnissen in die Datenbank VTED kann eine automatisierte Analyse von Testergebnissen und eine automatisierte Erstellung von Testberichten ausgeführt werden. Im einzelnen sind folgende Erweiterungen und Verbesserungen am VTC-Verfahren erarbeitet worden (vgl. Kapitel 6 und 7):

- Integration aller Testergebnisse ab 1997 in eine Datenbank
- Schneller Zugriff auf sämtliche Testergebnisse und vielfältige Sortiermöglichkeiten zur Datenausgabe
- Erstellung langfristiger Zeitreihen zu getesteten Qualitätskriterien
- Erstellung von grafischen Darstellungen der Testergebnisse
- Automatisierte Erstellung des VTC-Testberichtes
- Automatische Bewertung von Testergebnissen
- Vorgefertigte, automatisiert ausführbare Abfragen zu VTC-Testergebnissen

Ein regelmäßiger Import von den Ergebnissen zukünftiger Tests in die Datenbank VTED ist vorgesehen. Geplant ist, die Datenbank VTED und die erstellten Funktionalitäten bereits für die automatisierte Erstellung des Testberichtes des laufenden VTC-Tests (Veröffentlichung Herbst/Winter 2002) einzusetzen. In der Praxis wird sich zeigen, inwieweit dieser Prozeß

beschleunigt werden kann. Grafiken von Testergebnissen wurden bereits ab Test 2000-04 erstellt und sollen auch weiterhin erstellt werden.
Außerdem wird im VTC-Projektteam diskutiert, die Datenbank VTED zum Download auf der VTC-Webseite zur Verfügung zu stellen. Dies würde interessierten Besuchern der Webseite die Möglichkeit geben, gezielt auf sämtliche Testergebnisse des Virus Test Centers (ab 1997) zuzugreifen. Dagegen spricht die Gefahr eines Befalls der Datenbank mit Viren, die durch Makroviren bei einer Microsoft Access Datenbank generell gegeben ist. Das Virus Test Center hat eine besondere Verantwortung, solch einer Verbreitung von Viren vorzubeugen. Dies ist auch der Grund, warum die VTC-Testergebnisse bisher im ASCII-Format veröffentlicht werden, denn ASCII-Dateien enthalten keinen ausführbaren Code. Dementsprechend muß bei Einsatz der Datenbank zur Erstellung von Testberichten auch eine Entscheidung im Projekt für das Exportformat (*ASCII*, *rich text format* oder *html*) getroffen werden. Html-Export bietet die besten Gestaltungs- und Verlinkungsmöglichkeiten, birgt aber auch die größte Gefahr eines Befalls mit aktivem, maliziösem Code.

Neben dem Einsatz bei der Erstellung von Testberichten bietet die Integration sämtlicher Testergebnisse in eine Datenbank dem Benutzer noch eine Vielzahl von weiteren Möglichkeiten zur Analyse von Testergebnisdaten. Die vorliegende Arbeit stellt mit der Datenbank VTED eine Basis für die Programmierung von Datenbankabfragen zur Verfügung, mit denen verschiedene Statistiken der VTC-Testergebnisse erstellt werden können. So sind zum Beispiel Abfragen, die für jede Datenbank automatisch den Durchschnitt der Erkennungsrate mehrerer Tests pro Produkt ausgeben, denkbar. Dadurch könnte man die langfristig zuverlässigsten Produkte ermitteln. Aber auch genauere Betrachtungen anderer mitgetesteter Qualitätskriterien als der Erkennungsrate erscheinen interessant. Die in dieser Arbeit weiterentwickelte Datenbank VTED kann interessierten Studenten im VTC-Projekt als Basis für gezielte Untersuchungen von VTC-Testergebnissen dienen und so auch in Zukunft die Forschung auf diesem Gebiet als Werkzeug unterstützen.