5. Andere Tests von Anti-Malware-Software

In diesem Kapitel werden andere Institutionen, die Anti-Malware-Tests durchführen, kurz beschrieben (Abschnitt 5.1 bis 5.4) und mit dem VTC-Verfahren verglichen (Abschnitt 5.6). Dabei werden die getesteten Kriterien (entsprechend Kapitel 2) und die Qualität der Tests (entsprechend Kapitel 3) sowie insbesondere die Bewertung der Produkte betrachtet und verglichen. Zusätzlich werden das Vorgehen und die Qualität von Tests in Computerzeitschriften von den vorher vorgestellten Testeinrichtungen und dem Virus Test Center abgegrenzt (Abschnitt 5.5). Zum Abschluß des Kapitels folgt ein tabellarischer Vergleich der vorgestellten Testeinrichtungen und des VTCs hinsichtlich der jeweils getesteten (quantitativen) Kriterien und der Qualitätsrichtlinien für Anti-Malware-Tests (Abschnitt 5.6).

5.1 AV-Test.de

AV-Test.de ist eine Testinstitution, die in Zusammenarbeit der Otto-von-Guericke Universität Magdeburg mit der Firma Gega-IT Solutions unter der Leitung von Andreas Marx regelmäßig Tests von Anti-Malware-Software durchführt. Wie bei den VTC-Tests werden Vergleichstests mehrerer Produkte auf bestimmten Plattformen durchgeführt. Die Menge der bösartigen Softwareobjekte (Musterdateien) in den Datenbanken von AV-Test.de ist ähnlich umfangreich wie die der VTC-Datenbanken (vgl. Tabelle 5.A)[67]. Die Testmethodik und die angewendeten Verfahren zum Testen der Kriterien sind allerdings nicht dokumentiert.

Es wird eine große Anzahl an Vergleichstests von Anti-Malware-Produkten durchgeführt. In den einzelnen Tests werden sehr unterschiedliche Kriterien, Plattformen und Produkte getestet. Viele der Tests werden im Auftrag von Computerzeitschriften durchgeführt und richten sich deshalb bei den getesteten Kriterien nach den Wünschen der Auftraggeber. Einige Tests sind nach speziellen Gesichtspunkten ausgerichtet, wie der Erkennung von Schutzprogrammen für Groupware[68] oder serverbasierten Lösungen für die Erkennung bösartiger Software.

Da es sich um verschiedenartige Tests mit teilweise speziellen Themen und unterschiedlichen Zielsetzungen handelt, lassen sich keine generellen Angaben über den Aufbau, getestete Kriterien und Plattformen machen. Genaue Angaben zu AV-Test.de finden sich unter [AV-Test 2002a]; Tabelle 5.A (S. 91) zeigt einige Merkmale im Vergleich zum VTC und anderen Testeinrichtungen dieses Kapitels.

---

[67] Über die Herkunft und Qualität der Musterdateien in den Datenbanken sind keine Angaben verfügbar (vgl. [AV-Test 2002b]).

[68] beispielsweise *Microsoft Exchange* oder *Lotus Notes*

5.2 ICSA-Labs

ICSA-Labs ist eine kommerzielle Testinstitution, die gegen Entrichtung einer von Herstellerseite bezahlten Gebühr Testprodukte anhand festgelegter Kriterien zertifiziert. Die Testprodukte werden nicht untereinander verglichen. Entweder ein Produkt erfüllt die Kriterien und erhält das Zertifikat, oder es erfüllt die Kriterien nicht und erhält keine Zertifizierung.

Die Testmethodik und Inhalte der Datenbanken sind nicht öffentlich verfügbar. Lediglich die Testkriterien und die anhand dieser Kriterien zertifizierten Produkte werden veröffentlicht. Für Produkte, die nach einem Test kein Zertifikat erhalten haben, wird angegeben, welche Kriterien nicht erfüllt wurden. Dabei wird auch im Detail angegeben, welche Viren nicht erkannt wurden (*missed samples*), die Hersteller bekommen diese Dateien jedoch nicht zugeschickt.

Die Kriterien für Zertifizierungen sind folgende (siehe [ICSA-Labs 2002]):

Erkennung On-Demand Modus:

- 100% Erkennungsrate von *in-the-wild*-Viren[69]
- 100% Erkennungsrate von Viren in Datenbanken, die von ICSA als *häufige Infektoren* eingestuft werden
- 100% Erkennungsrate von polymorphen Viren
- 90% von Zoo-Viren in ICSA-Datenbanken
- keine Falschmeldungen (*false positives*)

Erkennung On-Access Modus:

- 100% Erkennungsrate von *in-the-wild*-Viren[69]
- 100% Erkennungsrate von Viren in Datenbanken, die von ICSA als *häufige Infektoren* eingestuft werden
- 90% von Zoo-Makro-Viren in ICSA-Datenbanken
- keine Falschmeldungen (*false positives*)

Reinigung:

- Reinigung von *in-the-wild*-Viren[69]
- Reinigung von Viren in Datenbanken, die von ICSA als *häufige Infektoren* eingestuft werden
- gereinigte Dateien dürfen nicht mehr replizieren
- gereinigte Dateien können geöffnet werden und auf enthaltene Daten kann zugegriffen werden
- gereinigte ausführbare Dateien behalten ihre Funktionalität

[69] entsprechend wildlist.org ([Wildlist 2002])

Neben diesen drei Zertifizierungen, die generell für Anti-Malware-Produkte anwendbar sind, gibt es weitere Zertifizierungen für Anti-Malware-Produkte in speziellen Anwendungsfeldern. Diese speziellen Anwendungsfelder sind:

- Internet Gateway E-mail
- Microsoft Exchange Server
- Lotus Notes
- Security Service Provider
- Internet Service Provider
- On-Line Anti-Virus Scanner

Nähere Angaben zu Anti-Malware-Zertifizierungen von ICSA-Labs finden sich in Tabelle 5.A (S. 91) oder unter [ICSA-Labs 2002].

5.3 West Coast Labs

Ähnlich wie ICSA ist West Coast Labs eine kommerzielle Testinstitution, die Produkte kostenpflichtig zertifiziert. Die Zertifizierungen für Anti-Malware-Produkte bei West Coast Labs heißen:

- Anti-Virus Checkmark Level 1
- Anti-Virus Checkmark Level 2
- Trojan Checkmark

Die Testmethodik und Inhalte der Datenbanken sind nicht öffentlich verfügbar. Lediglich die Testkriterien und die anhand dieser Kriterien zertifizierten Produkte werden veröffentlicht. Die Kriterien für die einzelnen Zertifizierungen lauten:

Anti-Virus Checkmark Level 1:
- 100% Erkennungsrate von *in-the-wild*-Viren[70]

Anti-Virus Checkmark Level 2:
- 100% Erkennungsrate von *in-the-wild* Viren[70]
- Reinigung von *in-the-wild*-Viren
  (die Datei muß nach der Reinigung ohne Verlust von Daten benutzbar sein)

Trojan Checkmark:
- 100% Erkennungsrate von Zoo-Malware in West Coast Labs Datenbanken
- keine Falschmeldungen (*false positives*)

Nähere Angaben zu Anti-Malware-Zertifizierungen von West-Coast-Labs finden sich in Tabelle 5.A (S. 91) oder unter [WestCoast-Labs 2002].

[70] entsprechend wildlist.org ([Wildlist 2002])

5.4 Virus Bulletin

Virus Bulletin ist eine Fachzeitschrift, die sich mit den Themen Computerviren und Malware beschäftigt. In der Zeitschrift werden Artikel und aktuelle Informationen zu bösartiger Software und Gegenmaßnahmen veröffentlicht. In diesem Zusammenhang führt die Zeitschrift auch regelmäßig Tests von Anti-Malware-Produkten durch, deren Ergebnisse in der Zeitschrift veröffentlicht werden.

Getestet wird die Erkennungsrate im *On-demand* Modus und im *On-access* Modus. Im Rahmen der Tests vergibt Virus Bulletin den sogenannten "VB100%-Award" (siehe [VirusBulletin 2002] und vgl. Kapitel 2, Abschnitt 2.2.7). Diesen Award erhalten pro Test jeweils die Produkte, die folgende Kriterien erfüllen:

VB100%-Award:

- 100% Erkennungsrate von *in-the-wild*-Viren im *On-demand* Modus[71]
- 100% Erkennungsrate von *in-the-wild*-Viren im *On-access* Modus[71]
- keine Falschmeldungen (*false positives*)

Genaue Testergebnisse werden in der Zeitschrift veröffentlicht; online wird lediglich angegeben, welche Produkte in welchem Test den "VB100%-Award" erhalten haben.

5.5 Tests von Antivirenprodukten in Computerzeitschriften

Neben den vorgestellten Testeinrichtungen, in denen Anti-Malware-Software nach jeweils festgelegten Kriterien getestet oder zertifiziert wird, testen auch viele Computerzeitschriften mit Heimanwendern als Zielgruppe[72] regelmäßig kommerzielle Antivirenprogramme, um dem Benutzer eine geeignete Produktauswahl zu ermöglichen (vgl. zum Beispiel [MarxBrauch 2001] und [PC Professionell 2002]). Diese Tests von Anti-Malware-Programmen in Computerzeitschriften unterscheiden sich in mehreren Punkten[73] von den vorgestellten Testeinrichtungen und dem VTC[74]:

- kleine Testmenge
- hohe Gewichtung qualitativer Kriterien
- keine Dokumentation des Testverfahrens
- mangelnde Qualitätssicherung der Testergebnisse

---

[71] entsprechend wildlist.org ([Wildlist 2002])

[72] im Gegensatz zu Fachzeitschriften wie Virus Bulletin, siehe 5.4

[73] vgl. [Klotz 2002]

[74] sofern der Test nicht im Auftrag einer Zeitschrift von einer der genannten Testinstitutionen durchgeführt wird

- subjektive Kommentare von Testern zu Produkten

Bei Tests in Computerzeitschriften werden häufig subjektive Bewertungen der Produkte durch Schilderungen von Eindrücken der Tester vorgenommen[75]. Ebenso geht auch die subjektive (nicht einer bestimmten Metrik folgende) Bewertung qualitativer Kriterien in die Gesamtbewertung der Produkte ein. Die Gewichtung der einzelnen Kriterien bei der Bewertung der Produkte ist höchst uneinheitlich (vgl. [Klotz 2002], S.6:"Almost every test uses different criteria, different levels of abstraction or different granularity of similar aspects.").

Die Implikationen aus wissenschaftlicher Sicht hinsichtlich der Ergebnisse solcher Tests sind eindeutig:

- keine Aussagekraft der Ergebnisse aufgrund kleiner Testmengen
- keine Nachvollziehbarkeit der Ergebnisse aufgrund ungenügender Dokumentation
- zweifelhafte Testergebnisse durch mangelnde Qualitätssicherung

Deshalb liefern Tests in Computerzeitschriften in der Regel[76] keine relevanten Ergebnisse und Produktbewertungen. Dennoch sind für die Benutzer die individuellen Eindrücke der Tester von Produkten hilfreich. Denn die Benutzbarkeit ist entscheidend für den tatsächlichen Schutz eines Sicherheitsmechanismusses (Charles Pfleeger in *Security in Computing*: "Controls must be used to be effective. They must be efficient, easy to use, and appropriate"; [Pfleeger 1997], S. 15). Gefällt ein Produkt einem Benutzer nicht, besteht die Gefahr, daß er es deaktiviert.

5.6 Vergleich anderer Anti-Malware Tests mit dem VTC Test

Tabelle 5.A vergleicht die angegebenen Tests von Anti-Malware-Software hinsichtlich getesteter Kriterien und Qualitätsrichtlinien für Anti-Malware-Tests entsprechend Kapitel 3. Die Tabelle liefert einen groben Überblick über die Unterschiede. Da die Tests fast ausschließlich quantitative Kriterien betrachten, wird auch nur das Testen dieser Kriterien in Tabelle 5.A verglichen. Jeder der Tests liefert nur eine Aussage in Bezug auf die getesteten Kriterien und die Qualität des Testverfahrens, somit sind die gelieferten Ergebnisse von unterschiedlicher Bedeutung und nicht einfach zu vergleichen.

[75]Karlhorst Klotz schreibt in seinem Vergleich von Anti-Viren-Tests in deutschen Computerzeitschriften: "Personal judgement transforms tests into reviews. This step is represented by the introduction of weights that allow for the calculation of a total performance that is based on single objective measurements or observations and subjective evaluations." ([Klotz 2002], S.6)

[76]sofern der Test nicht für eine Zeitschrift von einer der genannten Testinstitutionen durchgeführt wird

Test-Center / *Merkmale*	**Virus Test Center**	**AV-Test.de**	**ICSA Labs**	**West Coast Labs**	**Virus Bulletin**
Getestete Kriterien					
Erkennungsrate					
On-demand Modus	*ja*	*ja*	*ja*	*ja*	*ja*
On-access Modus	*nein*[a]	*ja*	*ja*	*ja*	*ja*
Erkennungsgenauigkeit	*ja*	*nein*	*nein*	*nein*	*nein*
Erkennungszuverlässigkeit	*ja*	*nein*	*nein*	*nein*	*nein*
Falschmeldungen	*ja*	*ja*	*ja*	*ja*	*ja*
Getestete Dateiformate					
exotische Plattformen	*ja*	*nein*	*nein*	*nein*	*nein*
komprimierte Dateien	*ja*	*ja*[b]	*ja*[b]	*nein*	*nein*
e-mails (MIME/uuencode)	*nein*	*ja*[b]	*ja*[b]	*nein*	*nein*
Geschwindigkeit	*nein*	*ja*	*nein*	*nein*	*ja*
Reparatur	*ja*	*ja*	*ja*	*nein*	*nein*
Qualität des Tests					
Testmenge					
Datenbanken[c]	• *ITW* • *Zoo*	• *ITW* • *Zoo*	• *ITW* • *Zoo*	• *ITW*	• *ITW* • *Zoo*
Größe	348695 infizierte Objekte[d]	342795 infizierte Objekte[e]	*?*	*?*	*?*
Qualität	*verschiedene Quellen und Qualitäts-sicherung*	*?*	*?*	*?*	*?*
Nachvollziehbarkeit der Ergebnisse	*detaillierte Angaben zur Test-Methodik online verfügbar*	*Test-methodik nicht online dokumentiert - nur die Testkriterien*	*Test-methodik nicht online dokumentiert - nur die Testkriterien*	*Test-methodik nicht online dokumentiert - nur die Testkriterien*	*Test-methodik nicht online dokumentiert - nur die Testkriterien*
Objektivität					
Herstellerunabhängigkeit	*ja*	*ja*	*ja*	*ja*	*bedingt*[f]
Kosten für Test	*kostenlos*	*kosten-pflichtig*	*kosten-pflichtig*	*kosten-pflichtig*	*kostenlos*
Aussagekraft der Ergebnisse					
Art der Bewertung	*Vergleich*	*Vergleich*	*Zertifikat*	*Zertifikat*	*Vergleich & Award*
Ergebnisse	*detailliert und nachvoll-ziehbar*	*detailliert*	*nur Zertifikat und Angabe von "missed samples"*	*nur Zertifikat*	*detaillierte Ergebnisse (nur in Zeitschrift)*

Tabelle 5.A: Vergleich von Testkriterien und Qualität ausgewählter Anti-Malware-Tests[77]

[77] Anmerkungen zur Tabelle auf der nächsten Seite

Anmerkungen zur Tabelle 5.A:

a - Ein On-Access Test ist im Virus Test Center in Planung, siehe [Siekierski 2002]

b - Die Kriterien werden nur unter bestimmten Plattformen oder für bestimmte Tests/Zertifizierungen getestet, in der Regel werden sie nicht getestet

c - Die Unterscheidung nach Itw- und Zoo-Datenbanken stellt nur eine grobe Einteilung dar, Details zu den Datenbanken sind entweder nicht verfügbar oder aufgrund unterschiedlicher Terminologie schwer zu vergleichen

d - Stand 30.04.2001, vgl. [VTC 2001-10a], 0execsum

e - Stand 18.12.2001, vgl. [AV-Test 2002b]

f - Das Magazin *Virus Bulletin* gehört zur selben Unternehmensgruppe wie die Software *Sophos-Anti-Virus* (vgl. [Bjergström 2001], S.1)

Das VTC-Verfahren unterscheidet sich von allen anderen Tests dadurch, daß das Testverfahren detailliert veröffentlich wird. Erst dadurch werden die Testergebnisse nachvollziehbar und wissenschaftlich relevant. Außerdem zeichnet das VTC-Verfahren aus, daß auch Erkennungszuverlässigkeit und -genauigkeit mitgetestet werden. Negativ fällt auf, daß alle anderen Tests die Erkennungsrate auch im *On-access* Modus testen, hier besteht Bedarf für Erweiterungen der VTC-Tests.

Ein weiteres Qualitätsmerkmal für die VTC-Tests ist die große Anzahl an Musterdateien in der Testmenge (siehe Größe unter Testmenge), die aussagekräftige Ergebnisse möglich macht. Bei den Testinstitutionen, die keine Angaben hierzu verfügbar machen, ist die Aussagekraft der Testergebnisse (wie der Erkennungsrate) zweifelhaft, zumindest bei Tests auf Zoo-Datenbanken. Ebenso zeichnet die VTC-Tests die für Hersteller kostenlose Teilnahme an den Tests aus, wodurch jedem Hersteller die Teilnahme ermöglicht wird und unabhängige Testergebnisse garantiert sind.

Nicht aus Tabelle 5.A ersichtlich - aber dennoch ein wichtiger Unterschied - ist die Tatsache, daß das VTC die einzige Testinstitution mit Grundsätzen zum Umgang mit bösartiger Software ist (VTC *code of conduct*, vgl. Kapitel 4, Abschnitt 4.1.1 und siehe Anhang A). Außerdem ist das VTC die einzige Testinstitution, die die Qualität von teilnehmenden Produkten[78] direkt durch das Zuschicken nicht erkannter Musterdateien (*missed samples*) verbessert.

[78] zumindest potentiell