2. Qualitätskriterien für die Erkennung von bösartiger Software

Um verschiedene Produkte zur Entdeckung und Entfernung von bösartiger Software (Anti-Malware-Produkte) hinsichtlich der Güte dieser Produkte zu vergleichen, ist es notwendig, Kriterien aufzustellen, durch die ein gutes Produkt gekennzeichnet sein sollte. Diese Kriterien dienen der objektiven Analyse und des Vergleichs mehrerer Anti-Malware-Produkte und sollen eine nachvollziehbare und wiederholbare Bewertung ermöglichen.

Zunächst werden Gesichtspunkte für die Qualität von Software im Allgemeinen untersucht (Abschnitt 2.1). Detaillierte Anforderungen speziell für Anti-Malware-Produkte werden unterschieden nach quantitativen (Abschnitt 2.2) und qualitativen (Abschnitt 2.3) Kriterien vorgestellt. Bei letzteren Kriterien ist zum Zeitpunkt des Entstehens dieser Arbeit keine Metrik bekannt, nach der eine Bewertung auf einer Zahlenskala vorgenommen werden kann. Eine exakte objektive Bewertung ist deshalb nicht immer möglich, da es sich um Eigenschaften handelt, die je nach Betrachter unterschiedlich wahrgenommen sowie bei der Bewertung unterschiedlich gewichtet werden. Bei quantitativen Kriterien besteht jedoch eine metrische Bewertungsskala, die eindeutig Ergebniswerte zu Messungen zuordnet. Beide - quantitative und qualitative - Kriterien beeinflussen die Qualität von Anti-Malware-Software; quantitative Kriterien lassen sich aufgrund vorhandener, allgemein akzeptierter metrischer Bewertungsschemata besser objektiv testen.

Der Vollständigkeit halber werden ferner Kriterien aufgeführt, die nicht im engeren Sinne zur Qualität eines Produktes beitragen, aber dennoch zur Unterscheidbarkeit der Eigenschaften von Anti-Malware-Produkten führen (Abschnitt 2.4). Sie eignen sich nicht gut für eine objektive Bewertung. Diese weiteren Aspekte beeinflussen im Einzelfall jedoch recht häufig die Kaufentscheidung des Konsumenten für das eine oder andere Produkt.

2.1 Allgemeine Qualitätsanforderungen an Software

Die Informatik-Literatur bietet ein weites Spektrum an Anforderungen, die an qualitativ gute Software zu stellen sind. So findet sich beispielsweise im Software-Engineering Buch von Pomberger und Blaschek folgende Auflistung ([PombergerBlaschek 1996], S. 9-13):

- Korrektheit
- Zuverlässigkeit
- Benutzerfreundlichkeit
- Wartungsfreundlichkeit
- Effizienz

- Portabilität

Der Informatik-Duden ([Informatik-Duden 1993], S. 655ff) nennt folgende Eigenschaften, die die Qualität eines Programms bestimmen:

- Benutzungsfreundlichkeit
- Zuverlässigkeit
- Wartbarkeit
- Anpaßbarkeit
- Portabilität
- Effizienz
- Ergonomie

Beide Auflistungen sind weitestgehend identisch. Pomberger und Blaschek listen zusätzlich die Korrektheit auf, weisen aber darauf hin, daß dieses Qualitätsmerkmal in der Praxis nicht immer leicht überprüfbar ist ([PombergerBlaschek 1996], S. 149f). Der Informatik-Duden nennt außer den Merkmalen aus dem Software-Engineering Buch noch Anpaßbarkeit, womit die leichte Anpassung an Benutzeranforderungen gemeint ist, und Ergonomie, welche man auch als Teilmenge der Benutzungsfreundlichkeit auffassen kann.

Einige dieser Kriterien, insbesondere Benutzerfreundlichkeit und Wartungsfreundlichkeit, lassen sich kaum objektiv mit einer Bewertungsskala bestimmen, bei der jeder Benutzer für die gleichen Produkte auf der Skala dieselben Werte benutzen würde. Beispielsweise kann ein Benutzer die Farbauswahl der grafischen Benutzeroberfläche eines Programms als gut erachten, während dieselbe Oberfläche einem anderen Benutzer unübersichtlich erscheint. Dies liegt daran, daß diese Kriterien in hohem Maße von der individuellen Sicht des Betrachters abhängen. Trotzdem kann man für diese Kriterien Eigenschaften festlegen, die nachvollziehbar meßbar sein können, so zum Beispiel die Menütiefe für die Benutzerfreundlichkeit oder die Anzahl der auszuführenden Schritte beim Update für die Wartungsfreundlichkeit. Obwohl die Fachdisziplin Softwareergonomie genau solche Kriterien entwickelt, sind dem Autor dieser Arbeit keine allgemein akzeptierten Bewertungsschemata für Benutzerfreundlichkeit und Wartungsfreundlichkeit von Anti-Malware-Software bekannt. Es handelt sich um qualitative Kriterien, welche bei der Evaluation und Messung von Softwareprodukten aufgrund der beschriebenen Subjektivität des Betrachters nur bewertet werden können, indem subjektive Entscheidungen begründet werden und anhand dieses Bewertungsschemas die Produkte betrachtet und bewertet werden (vgl. [Informatik-Duden 1993]. S. 90f). Die Effizienz hingegen läßt sich auf einer festgelegten Testplattform für verschiedene Produkte exakt bestimmen (etwa durch Zeitmessung und Angabe des Durchsatzes an Daten pro Zeiteinheit). Es handelt sich um ein quantitatives Kriterium, da eine metrische Bewertungsskala existiert.

Die erwähnten Kriterien dienen als Orientierungshilfen zur Bewertung von Software im allgemeinen. Will man Software nach der Eignung für eine spezielle Anwendung bewerten, so muß man für diese spezielle Anwendung ein spezielles Anforderungsprofil mit Kriterien

aufstellen und diese gewichten, damit man eine eindeutige Entscheidung treffen kann. Der Informatik Duden ([Informatik-Duden 1993], S. 91) schreibt hierzu: "Es empfiehlt sich jedoch, für jede Anwendung ein gesondertes Anforderungsprofil zu entwickeln und eine spezifische Bewertung vorzunehmen.".

Für die Bestimmung der Qualität von Anti-Malware-Produkten sind bestimmte, spezielle Kriterien von besonderer Bedeutung. Diese Kriterien bilden die Grundlage für die Bewertung der Erkennung von bösartiger Software und sollen im folgenden - unterschieden nach quantitativen und qualitativen Kriterien - erläutert werden.

2.2 Quantitative Kriterien für die Erkennung von bösartiger Software

Wie im vorigen Abschnitt beschrieben, muß, damit ein Softwareprodukt evaluiert werden kann, ein Anforderungsprofil an die Software entwickelt werden und in der Evaluation überprüft werden, inwieweit die Software diese Anforderungen erfüllt. Das Anforderungsprofil hat sich dabei an dem eigentlichen Zweck und der Zielsetzung der Software zu orientieren. Die Grundanforderungen an ein Anti-Malware-Produkt sind die Erkennung und Beseitigung von Malware zum Schutz eines Computersystems. Die in diesem und im nächsten Abschnitt aufgezählten Kriterien helfen bei der Evaluation, da man von ihrer Ausprägung die Erfüllung der Anforderungen ableiten kann.

Quantitative Kriterien zur Feststellung der Qualität eines Anti-Malware-Produktes für den Benutzer sind:

- Erkennungsrate
- Erkennungsgenauigkeit
- Erkennungszuverlässigkeit
- Häufigkeit von Falschmeldungen
- Unterstützung von Datenformaten
- Geschwindigkeit
- Reparatur von infizierten Dateien

Die Aussagekraft dieser Kriterien über ein Produkt und die Bedeutung zur Erkennung bösartiger Software wird in den folgenden Unterabschnitten genauer beschrieben.

2.2.1 Erkennungsrate

Die Erkennungsrate, mit der ein Anti-Malware-Produkt bösartige Software erkennt, ist zweifelsohne das wichtigste quantitative Kriterium für die Qualität eines getesteten Produktes. Denn die eigentliche Kernanforderung an ein Anti-Malware-Produkt ist die Erkennung von bösartiger Software, und die Qualität dieser Erkennung wird durch die Erkennungsrate entscheidend wiedergegeben.

Mit der Erkennungsrate sind die aus einer bestimmten Menge an Malwaredateien als Malware erkannten Dateien gemeint. Diese Rate wird meist prozentual angegeben und bezeichnet den Prozentsatz, den ein bestimmtes Produkt aus einer Menge von bösartiger Software erkannt hat. Die Erkennungsrate berechnet sich nach der simplen Formel:

$$E = \frac{dm}{tb}$$

E: Erkennungsrate
dm: detected malware (dt. gefundene Malware)
tb: testbed (gesammte Menge an Malware)

Die Erkennungsrate bezieht sich dabei auf eine bestimmte Datenbank[20] von Viren/Malware, und gibt an, wieviele Dateien aus der jeweiligen Datenbank erkannt wurden. Die Datenbanken können zum Beispiel nach Plattform oder Verbreitung (vgl. Kapitel 1.2) sortiert sein. So kann eine detaillierte Aussage darüber gemacht werden, wo ein Anti-Viren-Scanner gut in der Erkennung von Malware ist und wo er Schwächen aufzeigt, da die Erkennungsrate differenziert für jede Datenbank angegeben wird.

Für eine Datenbank muß angegeben werden, welche Art von Viren in ihr enthalten sind und ob es sich um *in-the-wild*-Viren oder um Zoo-Viren handelt. Zusätzlich muß bei der Erkennungsrate noch unterschieden werden, ob es sich um die Rate eines Produktes im *On-demand*-Betrieb oder im *On-access*-Betrieb handelt, da sich die Erkennungsraten bei beiden Betriebsarten eines Anti-Malware-Produktes erfahrungsgemäß unterscheiden können. Je genauer sich die Erkennungsrate auf eine bestimmte Klassifikation von Viren/Malware bezieht, desto besser ist die gewonnene Aussage über die Erkennung dieser Klasse von Viren/Malware.

2.2.2 Erkennungsgenauigkeit und -zuverlässigkeit

Ein die Erkennungsrate erweiterndes Qualitätskriterium ist die Zuverlässigkeit der Erkennung von Malware. Die Erkennungsrate sagt lediglich aus, wieviel Prozent an maliziösen Objekten bzw. Viren von allen maliziösen Objekten/Viren in einer bestimmten Datenbank vom Scanner erkannt wurden. Wünschenswert ist jedoch zudem eine zuverlässige Erkennung von dem Scanner bekannten Viren. Mit zuverlässiger Erkennung ist gemeint, daß ein Scanner jede Musterdatei eines ihm bekannten Virus erkennt. Diese Anforderung erscheint logisch, ist aber in der Praxis nicht immer gegeben. Da zum Beispiel polymorphe Viren ihren eigenen Code bei jeder Infektion leicht verändern, ist es nicht selbstverständlich, daß ein Scanner, der einen derartigen Virus in einer infizierten Datei erkennt, diesen Virus in allen infizierten Dateien erkennt.

[20] mit Datenbank ist in diesem Zusammenhang keine relationale Datenbank gemeint, sondern lediglich eine Sortierung von Malware nach Klassifikation in einem Dateisystem (siehe Abschnitt 1.2)

Außerdem ist von einem Virenscanner eine konstante Bezeichnung von Malware zu erwarten. In den letzten Jahren kann beobachtet werden, daß immer mehr Anti-Malware-Hersteller dazu übergehen, verschiedene Varianten eines Virus nur noch generisch zu identifizieren[21]. Einem solchen Produkt mangelt es an Genauigkeit der Identifizierung. Für den Benutzer ist das negativ, da er auf diversen Webseiten (zum Beispiel [NAI-VirusLibrary 2002]) zwar nachlesen kann, wie sich eine bestimmte Variante eines Virus verhält und welchen Schaden sie anrichtet, er bei generischer Erkennung aber nicht weiß, welche Variante er sich eingefangen hat. Er muß sich in diesem Fall voll und ganz auf die Entfernungsroutine des Virenscanners zur Beseitigung des Virus verlassen. Aber eine saubere Entfernung ist in der Praxis keinesfalls bei allen Produkten gegeben (vgl. [RetschTode 2000], S. 207-240).

Deshalb ist eine genaue, zuverlässige Identifizierung eines Malwareobjektes eine Anforderung an Anti-Malware-Software. Sie wird beispielsweise bei den Tests des VTC auf folgende Weise mit aufgelistet ([VTC 2001-10a], 5protoco.txt):

- "The number of viruses with unreliable (=inconsistent) identification: all variants of a viruses are detected but at least one sample is identified with a different name." (Genauigkeit)
- "The number of viruses with unreliable detection: here, not all samples of a virus are detected but at least one." (Zuverlässigkeit)

2.2.3 Häufigkeit von Falschmeldungen

Eine hohe Erkennungsrate kann unter Umständen von Anti-Malware-Programmen dadurch erreicht werden, daß diese bereits bei geringem Verdacht auf bösartige Software einen Alarm melden. So wird zwar die Erkennungsrate gesteigert, aber für einen Benutzer (der die Bösartigkeit einer Datei anders als durch den Scanner nicht einschätzen kann und somit diesem vertraut) besteht so die Gefahr, daß er saubere Dateien löscht, weil sie vom Anti-Malware-Programm als Malware identifiziert wird. Auch wenn die Erkennung von bösartiger Software die Hauptanforderung an Anti-Malware-Software stellt, ist dieser Effekt doch unerwünscht.

Deshalb ist es zweckmäßig, auch die Zahl der falsch als bösartige Software gemeldeten Dateien (sogenannte *false positives*) zu messen. Dies geschieht in der Regel dadurch, daß in die Datenbanken saubere Dateien in zufällig gewählten Verzeichnissen eingefügt werden, die von den Scannern dann als sauber gemeldet werden müssen.

[21] Benennt ein Antivirenprogramm jede gefundene Variante eines bestimmten Virus oder anderer Malware mit der gleichen Bezeichnung spricht man von generischer Erkennung.

2.2.4 Unterstützung von Dateiformaten

Da ein Virenscanner möglichst alle Malware entdecken soll, ist es wichtig zu testen, ob ein Produkt alle Arten von Dateitypen lesen und prüfen kann. Insbesondere Komprimierungsprogramme und die von ihnen erzeugten komprimierten Dateien müssen von einem Virenscanner unterstützt werden, da sonst Viren in gepackten[22] Archiven unentdeckt auf den zu schützenden Rechner gelangen können. Diese Unterstützung von Dateiformaten unterschiedlicher Komprimierungsprogramme stellt insofern eine Schwierigkeit für die Hersteller von Virenscannern dar, als daß der Viruscode in einer komprimierten Datei ebenfalls in komprimierter, also veränderter Form vorliegt. Der Virenscanner muß also zur Erkennung das entsprechende Komprimierungsformat kennen, die Datei entpacken, und dann die entpackte Datei auf bekannte Signaturen prüfen.

Eine Vielzahl von Komprimierungsprogrammen zum Archivieren und Komprimieren von Dateien existiert[23]; am meisten verbreitet sind folgende Formate (angegeben ist die Dateiendung, vgl. [Freitag 2000], S.30):

- für Windows-Systeme: .zip, .lha, .arj, .rar, .ace
- unter Unix und Linux: .tar, .taz, .z, .gz

Um die Erkennung von Malware in komprimierten Dateien unterschiedlichen Formats testen zu können, müssen lediglich Samples von Viren mit verschiedenen Programmen gepackt werden und diese gepackten Dateien dann in die Testdatenbank integriert werden.

Außer komprimierten Dateien müssen Anti-Malware-Programme auch Dateiformate anderer Plattformen und Betriebssysteme als die, auf denen die Anti-Malware-Software lauffähig ist, erkennen. Diese Erkennung "fremder" Dateiformate ist deshalb wichtig, weil so auch die Verbreitung von Malware verhindert werden kann, die auf dem System, auf dem die Anti-Malware-Software installiert ist, gar nicht lauffähig ist (und somit dort auch keinen Schaden anrichten kann). Trotzdem werden diese Dateien sonst eventuell via e-mail oder Internet-Protokollen, durch die auch Rechner mit anderen Betriebssystemen auf das System zugreifen können (wie zum Beispiel ftp oder telnet), weiterverbreitet.

Hinzu kommt, daß viele Anti-Malware-Produkte auf Gateway-Rechnern installiert sind, die e-mails und Pakete anderer Protokolle auf dem Weg aus einem Netzwerk ins Internet und umgekehrt durchsuchen. Bei einer derartigen Installation ist klar, daß der Virenscanner nicht nur Malware erkennen soll, die auf dem Gateway-Rechner lauffähig ist und funktioniert, sondern Malware aller Plattformen und Betriebssysteme, die im dahinter liegenden Netzwerk angeschlossen sind.

---

[22] *gepackt* ist ein gebräuchliches Synonym für *komprimiert*

[23] eine Übersicht findet sich unter [Compression-FAQ 2002] und [ACT 2002]

2.2.5 Geschwindigkeit

Gerade bei dem am Ende des vorigen Abschnittes angesprochenen Einsatz auf Gateways, die ein großes, internes Netzwerk mit dem Internet verbinden, ist die Geschwindigkeit des Scannens von Dateien ein zusätzliches Entscheidungskriterium. In vielen großen Unternehmen werden beispielsweise auf die beschriebene Art mehrere Tausend e-mails pro Tag nach Malware gescannt, damit das Unternehmensnetzwerk nicht befallen wird. Soll die für das Unternehmen ebenso wichtige elektronische Kommunikation dennoch zügig ablaufen, so ist ein schnelles Scannen der Dateien vonnöten. Viele Hersteller von Virenscannern empfehlen sich daher den Unternehmen durch die Aussage, ihre Produkte seien extrem schnell, da dies für die Unternehmen als Kunden ein wichtiges Entscheidungskriterium ist.

Da aufgrund der - zum Signaturenvergleich notwendigen - Speicherzugriffe beim Virenscannen ein gewisser Trade-Off zwischen Geschwindigkeit auf der einen Seite und Erkennungsrate sowie Erkennungsgenauigkeit auf der anderen Seite besteht, ist eine Aussage über die Geschwindigkeit eines Virenscanners nur sinnvoll in Zusammenhang mit der dabei erzielten Erkennungsrate. Ein schneller Virenscanner, der nur wenige Viren erkennt, ist von keinem Nutzen. Deshalb kann die Geschwindigkeit nur zusätzlich zu einer ausreichend guten Erkennungsrate ein Qualitätskriterium sein.

2.2.6 Reparatur von infizierten Dateien

Die Erkennung von bösartiger Software steht für Anti-Malware-Software im Vordergrund, damit so die Ausführung oder bereits das Kopieren von Malware verhindert wird. Sind aber erst einmal Dateien auf einem Rechner infiziert und wird dies im Nachhinein von Anti-Malware-Software erkannt, so muß diese die Malware auch entfernen können. Diese Fähigkeit ist besonders entscheidend, wenn die befallen Dateien wichtige Daten enthalten, und somit ein Löschen der maliziös verseuchten Dateien nicht in Frage kommt.

Besonders bei Makro-Viren stellt das korrekte Entfernen von Malware und die Wiederherstellung des Originalzustandes von Dateien eine hohe Anforderung an ein Anti-Malware-Produkt (vgl. [RetschTode 2000], S. 33-34). Beschränkt sich die Erkennung in der Regel auf den Vergleich von Signaturen und das Überwachen von Aktivitäten, so sind bei der Entfernung der inverse Vorgang des Virenbefalls und alle an der befallenden Datei durch den Virus vorgenommenen Änderungen durchzuführen. Trotz dieser höheren Schwierigkeit ist eine Aussage über die Fähigkeit zur Reparatur von infizierten Dateien ein wichtiges Qualitätskriterium für Anti-Malware-Software.

2.2.7 Beispiele

In der Praxis werden unterschiedliche quantitative Kriterien an Anti-Malware-Produkte aufgestellt und teilweise auch gewichtet. Die folgenden beiden Beispiele sollen verdeutlichen, welche Kriterien in welchem Maße bei unterschiedlichen Anti-Malware-Tests zum Ergebnis

beitragen. Beispielhaft sind dafür die Kriterien vom Virus Test Center für ein *perfect anti-virus product* bzw. ein *perfect anti-malware product* (siehe z.B. [VTC 2001-10a], 7evalwnt.txt) sowie die Kriterien für den *VB 100% Award* von Virus Bulletin (siehe [VirusBulletin 2002]) angegeben.

Beide Tests haben unterschiedliche Anforderungen für ihre Scanner-Bewertungen. In Kapitel 3 werden Qualitätsrichtlinien zur Bewertung und Aussagekraft von Anti-Malware-Tests genauer untersucht.

Virus Test Center Universität Hamburg

Die Kriterien des Virus Test Center für ein perfektes AntiVirus-Produkt (siehe Abb. 2.A) fordern für einen "perfekten" Virenscanner:

- 100% Erkennungsrate bei ITW-Viren (on demand)
- 99,9% Erkennungsrate bei Zoo-Viren (on demand)
- 100% Erkennungsrate von ITW-Viren, die mit 6 verschiedenen Komprimierungsprogrammen gepackt worden sind (PKZIP, LHA, ARJ, RAR, WinRAR, CAB)
- Keine einzige Falschmeldung

Definition (1): A "Perfect AntiVirus (AV) product"
---

1) Will detect ALL viral samples "In-The-Wild"
AND in at least 99.9% of zoo samples,
in ALL categories (file, boot and script-based viruses), with always same high precision of identification and in every infected sample,
2) Will detect ALL ITW viral samples in compressed objects for all (6) popular packers, and
3) Will NEVER issue a False Positive alarm on any sample which is not viral.

Abbildung 2.A: Kriterien für ein "Perfect AntiVirus (AV) product" vom Virus Test Center Hamburg[24]

Die Kriterien des Virus Test Center für ein "perfektes" AntiMalware-Produkt (siehe Abb. 2.B) fordern für einen (auch auf die Erkennung von nichtviraler Malware bezogen) "perfekten" Virenscanner:

- 100% Erkennungsrate bei ITW-Viren (on demand)

[24]siehe [VTC 2001-10a], 7evalwnt.txt

- 99,9% Erkennungsrate bei Zoo-Viren (on demand)
- 100% Erkennungsrate von ITW-Viren, die mit 6 verschiedenen Komprimierungsprogrammen gepackt worden sind (PKZIP, LHA, ARJ, RAR, WinRAR, CAB)
- Keine einzige Falschmeldung
- 90% Erkennungsrate bei sonstiger Malware

Definition (2): A "Perfect AntiMalware (AM) product"
---
1) Will be a "Perfect AntiVirus product",
That is: 100% ITW detection
AND >99% zoo detection
AND high precision of identification
AND high precision of detection
AND 100% detection of ITW viruses
in compressed objects,
AND 0% False-Positive rate,
2) AND it will also detect essential forms
of malicious software, at least in unpacked
forms, reliably at high rates (>90%).

Abbildung 2.B: Kriterien für ein "Perfect AntiMalware (AM) product" vom Virus Test Center Hamburg[25]

Virus Bulletin

Um von der Fachzeitschrift Virus Bulletin den *VB 100% Award* (siehe Abb. 2.C) verliehen zu bekommen, muß ein Virenscanner folgende Bedingungen erfüllen:

- 100% Erkennungsrate bei ITW-Viren (on demand)
- 100% Erkennungsrate bei ITW-Viren (on access)
- Keine einzige Falschmeldung

"The VB 100% logo is awarded to products that detect all In the Wild viruses during both on-demand and on-access scanning in Virus Bulletin's comparative tests. The product must also produce no false positives."

Abbildung 2.C: Kriterien für den "VB 100% Award" von Virus Bulletin[26]

[25]siehe [VTC 2001-10a], 7evalwnt.txt
[26]siehe [VirusBulletin 2002]

2.3 Qualitative Kriterien für die Erkennung von bösartiger Software

Folgende Kriterien müssen bei der qualitativen Betrachtung der Qualität von Anti-Malware-Produkten beachtet werden (vgl. auch [Bjergstrom 2001], S.25):

- Bedienbarkeit
- Benutzerfreundlichkeit
- Stabilität
- Funktionalität
- Korrektheit
- Anpaßbarkeit
- Wartungsfreundlichkeit
- Administrierbarkeit und -aufwand

Zeichnen sich quantitative Kriterien, wie im vorangegangenen Abschnitt vorgestellt, durch eine objektive und eindeutig nachvollziehbare Bewertung unter einer festgelegten Metrik aus, so sind qualitative Kriterien in der Regel sowohl in der Bewertung als auch in der Einschätzung der Wichtigkeit subjektiven Vorstellungen unterworfen. Dennoch sind diese Kriterien für private Benutzer und Unternehmen oft ausschlaggebende Kaufkriterien. Dies liegt auch daran, daß diese Gesichtspunkte teilweise bei der Betrachtung der Produkte - zumindest oberflächlich - leicht anzuschauen sind. So bekommt man beispielsweise als Benutzer schnell einen Einblick in die Bedienbarkeit eines Programms. Trotzdem sind gerade diese Kriterien für die Qualität eines Anti-Malware-Produktes nicht leicht gründlich zu testen und zu messen, da Probleme oft im Detail und versteckt liegen (vgl. [Bjergstrom 2001], S.25: "it is my experience that even the more obvious purchase decision parameters are difficult to evaluate when it comes to choosing anti-malware protection").

Die aufgezählten qualitativen Kriterien tragen eher indirekt zur Erfüllung der Anforderung (also der Erkennung von Malware) bei. Trotzdem ist die Qualität hinsichtlich dieser Kriterien entscheidend für den erfolgreichen Einsatz von Anti-Malware-Software. Randy Abrams, Anti-Virenspezialist von Microsoft, nennt vier Fehlerquellen, bei deren Vorliegen Anti-Viren-Software nicht erwartungsgemäß funktioniert ([Abrams 2001], S.2):

- software bug (↦ Korrektheit)
- software conflict (↦ Anpaßbarkeit, Korrektheit)
- user interface issue (↦ Bedienbarkeit)
- user attention to detail (↦ Benutzerfreundlichkeit)

Diese Ursachen für Probleme bei Anti-Viren-Software können durch entsprechende Ausprägungen der in Klammern genannten Qualitätsmerkmale vermieden werden. Da die aufgezählten Probleme häufige Ursachen für Fehlverhalten in Anti-Virus-Software sind (vgl. [Abrams 2001]), sind die in Klammern genannten Kriterien entscheidend für die Qualitätsbestimmung eines Anti-Malware-Produktes.

2.3.1 Bedienbarkeit und Benutzerfreundlichkeit

Die Aspekte der Bedienbarkeit eines Anti-Malware-Produktes unterscheiden sich nicht wesentlich von denen für andere Softwareprodukte. Entscheidend für eine gute Bedienbarkeit sind das Design, die Menüführung und die Ergonomie (vgl. [PombergerBlaschek 1996], S. 66-81) der grafischen Oberfläche. Unterschieden werden kann in diesem Zusammenhang nach der Ausführung eines Programms über eine grafische Oberfläche (GUI für "grafical user interface") oder über eine Kommandozeile (CLI für "command line interface"). Letztere eignet sich insbesondere für den automatisierten Betrieb. Eine gute Benutzerfreundlichkeit wird geboten durch intuitive Menüpunkte, transparente Befehle (d.h., dem Benutzer wird deutlich, was die Befehle bewirken) und durch eine gute Hilfe des Programms. Eine übersichtliche und ausführliche Dokumentation trägt ebenfalls zu einem benutzerfreundlichen Programm bei.

Gute Bedienbarkeit und Benutzbarkeit sind ausschlaggebend für die Sicherheit eines Anti-Malware-Produktes. Nur mit den richtigen Einstellungen kann der optimale Schutz gewährleistet werden. Randy Abrams schreibt in diesem Zusammenhang: "... better user interface designs and attention messages can greatly enhance the defensive value of the software" ([Abrams 2001], S.1). Oftmals sind wichtige Features in Untermenüs versteckt, oder Optionen werden irrtümlich gewählt, da die Bedeutungen von Funktionen dem Benutzer nicht klar aufgezeigt werden.

2.3.2 Stabilität

Die Stabilität ist für ein Anti-Malware-Produkt äußerst wichtig, da ein abgestürzter Scanner entweder einen wichtigen Gateway-Rechner blockieren kann oder - im schlimmeren Fall - das System ohne den Schutz des Scanners weiterläuft und so ungescannte Dateien vom Benutzer ausgeführt werden. Letztere Situation ist fatal im Falle eines im Hintergrund aktiven On-Access Scanners, der alle Dateien vor dem Öffnen prüft. Denn standardmäßig geben Scanner im On-Access-Modus meist keine Meldungen bei Dateien ohne gefundene Malware aus, sondern lassen diese regulär vom Betriebssystem ausführen, so daß im Falle eines Absturzes des On-Access-Scanners für den Benutzer die Datei geprüft und sauber erscheint, aber in Wahrheit gar nicht geprüft wurde. Zur Erkennung von Malware ist also eine stabile Software unabdingbar. Nur durch Stabilität der Anti-Malware-Software kann Sicherheit gewährleistet werden.

2.3.3 Funktionalität

Mit Funktionalität bezeichnet man die einzelnen "Features" und Optionen, die ein Softwareprodukt dem Benutzer bietet. Eine größere Anzahl an Funktionen ist nicht unbedingt besser als eine geringe Anzahl; letztere bietet in der Regel mehr Übersichtlichkeit. Vielmehr muß die Funktionalität den Anforderungen an Anti-Malware-Software in ausreichendem Maße gerecht werden. Um so adäquater die Funktionen hinsichtlich Bedienbarkeit, Benutzerfreundlichkeit, Anpaßbarkeit, Wartungsfreundlichkeit und Administrierbarkeit die

Anforderungen an ein Anti-Malware-Produkt erfüllen, desto besser ist die Qualität der Funktionalität der Software.

Die Funktionen finden sich meistens in den Menüs und Untermenüs eines Programms, bei Ausführung über die grafische Oberfläche, oder als sogenannte "switches" (dt. Eingabeparameter) bei der Ausführung über die Kommandozeile.
Typische Funktionen von Anti-Malware-Software sind (um nur einige wichtige zu nennen):

- das Aktivieren der Protokollfunktion und Festlegen von diversen Einstellungen zu Name, Länge, Format und Speicherort von Protokolldateien
- die Einstellung der Intensität der heuristischen Suche nach Viren; mit einer besseren Heuristik sinkt in der Regel die Geschwindigkeit des Scanners
- Einstellungen zum Herunterladen von Updates (Frequenz, automatisches Herunterladen oder nicht)
- die Angabe von zu scannenden Objekten, zum Beispiel ein Scan aller Dateien, oder nur von bestimmten Dateitypen
- Einstellungen zum Scannen von komprimierten Dateien (Entkomprimierungstiefe, unterstützte Formate)
- Einstellungen betreffend des Verhaltens des Scanners bei Fund von bösartiger Software (Ignorieren, Löschen, Isolieren, Warnmeldung)

2.3.4 Korrektheit

Die vom Hersteller eines Produktes angegebene Funktionalität ist nur dann ein Merkmal für die Qualität dieses Produktes, wenn alle angegebenen Funktionen korrekt funktionieren. Formal ist die Korrektheit von Programmen im Informatik-Duden definiert ([Informatik-Duden 1993], S. 762):

> "Ein Programm heißt korrekt, wenn es genau die vorgegebene Spezifikation erfüllt, also auf alle Eingaben mit den gewünschten Ausgaben reagiert"

Korrektheit heißt also, daß Funktionen in einem Programm das Erwartete tun, und in diesem Sinne "korrekt" funktionieren. Die Korrektheit ist eine Anforderung an jegliche Art von Software, da nur durch die korrekte Funktion ein sinnvoller Einsatz von Software möglich wird. Sonst stünden unvorhersehbare Ausgaben den Eingaben gegenüber. Bei Sicherheitssoftware, und im speziellen Anti-Malware-Software, ist die Korrektheit von besonderer Bedeutung, weil von ihr der Schutz des Systems abhängt. Der Benutzer nimmt bestimmte Einstellungen vor und verlässt sich bei der Ausführung des Programms auf die korrekte Anwendung dieser Einstellungen.

2.3.5 Anpaßbarkeit und Wartungsfreundlichkeit

Für die Anpaßbarkeit von Anti-Malware-Produkten spielen folgende Funktionen eine Rolle:

- Erstellen von Benutzerprofilen
- Möglichkeit zum Speichern der Einstellungen
- Möglichkeiten, die gebotenen Funktionen ein- und auszuschalten
- Anpassung an die Systemumgebung (insbesondere ein Netzwerk)
- Möglichkeit zur ferngesteuerten Ausführung (in Netzwerken)
- Möglichkeiten zur Planung und zeitlichen Ausführung von Ereignissen

Die Wartung von Anti-Malware-Produkten betrifft insbesondere das Herunterladen von Updates (Signaturen und Engines, vgl. Kapitel 1.2). Dieses kann manuell (der Benutzer muß das Herunterladen von Updates selber ausführen und diese von Hand installieren) oder automatisch (das Programm lädt Updates von selbst herunter und installiert sie) erfolgen. Eine automatische Wartung ist zu bevorzugen, dennoch sollte ein Programm die Option besitzen, die automatische Wartung abzuschalten, und das manuelle Installieren von Updates erlauben.

2.3.6 Administrierbarkeit und -aufwand

Jegliche Form von IT-Sicherheit ist nur nützlich, wenn sie auch benutzt wird. Charles Pfleeger schreibt dazu: "...computer security controls must be efficient enough, in terms of time, memory space, human activity, or other resources used, so that using the control does not seriously affect the task being protected" ([Pfleeger 1997], S. 15). In dieser Hinsicht ist eine einfache und nicht zeitaufwändige Administrierbarkeit eines Anti-Malware-Produktes notwendig, da sonst die Gefahr besteht, daß die Funktionen der Software nicht richtig genutzt werden und das System somit nicht ausreichend geschützt ist. Die optimale Erkennungsrate eines Scanners kann nur erreicht werden, wenn die Software der Umgebung und den Anforderungen entsprechend eingestellt ist, und wenn regelmäßig Updates von Signatur und Engine vorgenommen werden.

Ungenügende Administration und falsche Einstellungen können fatale Folgen für die Sicherheit durch Anti-Malware-Programme haben (vgl. [Abrams 2001]). Darum ist eine gute Administration der Software essentiell für das Erreichen eines optimalen (durch die Software gebotenen) Schutzes. Solch eine Administration kann nur durch eine übersichtliche, intuitive Administrierbarkeit mit vertretbarem Aufwand erreicht werden. Eine gute Administrierbarkeit wird erreicht durch eine entsprechende Funktionalität in Zusammenhang mit guter Anpaßbarkeit und Bedienbarkeit des Produktes.

2.3.7 Beispiel

Ein Beispiel für die Bewertung von qualitativen Kriterien ist der Test von Antivirenprogrammen in der Computerzeitschrift *c't* (Ausgabe 2001/2). In diesem Test

(siehe [MarxBrauch 2001]) gingen neben quantitativen Kriterien[27] folgende Gesichtspunkte mit in die Produktbewertung ein:

- Bedienung
- Konfiguration
- Funktionsumfang
- Dokumentation

Die aufgelisteten Aspekte betreffen die qualitativen Kriterien Bedienbarkeit, Benutzerfreundlichkeit und Funktionalität. Diese einzelnen Punkte wurden jeweils zusammenfassend mit [++] für sehr gut bis [--] für sehr schlecht bewertet. Eine Gesamtbewertung mit Gewichtung der einzelnen Kriterien wurde nicht vorgenommen. Wie die Bewertungen im einzelnen entstehen, ist nicht ersichtlich.

2.4 Andere Kriterien

Die in den beiden vorangegangenen Abschnitten (2.2 und 2.3) vorgestellten Kriterien bestimmen die Qualität von Anti-Malware-Software im eigentlichen Sinne, weil sie die Kernanforderung, nämlich die korrekte Erkennung und Entfernung von bösartiger Software, beeinflussen. Es gibt aber auch andere Kriterien, die nicht direkt zur Erfüllung der Hauptanforderung von Anti-Malware-Software beitragen, aber dennoch für den Benutzer von Wichtigkeit sein können. Ferner lassen sich diese Kriterien nicht sinnvoll testen, deshalb sollen sie an dieser Stelle nur der Vollständigkeit aufgezählt und kurz erläutert werden:

- Preis
- moralische Gesichtspunkte
- Support

Der Preis ist zwar ein quantitatives Kriterium, aber er steht in keinem Verhältnis zur Qualität eines Produktes (Niels-Jorgen Bergstrom: "... and there is no correlation between price and quality ... quite amazing, really, if you consider that we have had anti-virus products for 15 years now", [Bjergstrom 2001], S. 25). Dennoch ist er ausschlaggebend für den Kauf eines Produktes, sowohl für private Benutzer als auch für Firmen. Dies kann kurzsichtig sein, denn ein minderwertiges Produkt zieht oft unvorhersehbare Folgekosten nach sich, im Zweifelsfall sogar durch den durch nicht erkannte Malware angerichteten Schaden.

Ein Beispiel soll die Bedeutung moralischer Gesichtspunkte bei der Beurteilung von Anti-Malware-Produkten verdeutlichen. Seit kurzer Zeit gibt es ein neues Anti-Viren-Produkt mit dem Namen Open-Antivirus ([OpenAntivirus 2002]). Dieser Scanner bedient sich der Arbeit anderer Hersteller, indem er seine Signaturen unter Benutzung anderer

[27] Erkennungsrate, Desinfektionsleistung (Reparatur), Geschwindigkeit

Anti-Malware-Produkte erstellt. Jeder Benutzer der Software Open-Antivirus kann, sofern er einen anderen Scanner zur Erkennung von Malware installiert hat, zu von diesem anderen Scanner erkannten bösartigen Softwareobjekten Signaturen für Open-Antivirus erstellen (eine genaue Beschreibung des Verfahrens, dem sogenannten *pattern finder*, findet sich unter [OpenAntivirus PF 2002]). Das von Open-Antivirus angewandte Verfahren mag rechtlich in Ordnung sein. Das beschriebene Vorgehen ist allerdings bedenklich, da sich Open-Antivirus ohne Gegenleistung (zum Beispiel in Form von Nutzungsgebühren) und ohne Einwilligung seitens der anderen Hersteller die zeitintensive Arbeit anderer zur Erstellung von Signaturen - durch kostenintensive Laborteams - zunutze macht. Unabhängig von der durch die Kumulation von Signaturdateien durch Benutzung anderer Virenscanner erreichten Erkennungsrate gibt es ethische Gründe, namentlich die Ablehnung von Diebstahl und das Gebot der Fairneß, das Produkt Open-Antivirus nicht zu untersuchen oder für den Einsatz in Betracht zu ziehen. Solche Gesichtspunkte sind Sonderfälle, die im Einzelfall betrachtet werden müssen und nicht getestet oder gemessen werden können. Aggressives Marketing, bei dem ein Hersteller andere Konkurrenten unfair behandelt, ist ein weiteres Beispiel für moralische Überlegungen, die ein Kriterium für die Beurteilung einer Anti-Malware-Software darstellen können.

Der Herstellersupport einer Software kann die Zufriedenheit des Kunden mitunter sehr beeinflussen. Der Support trägt aber nur sehr indirekt zur Qualität der Erkennung von bösartiger Software bei. Außerdem ist er nur durch Stichproben (etwa Anrufe mit vorgetäuschten Problemen) zu testen.