www.virenspezialist.com

E-BOOK
RATGEBER

VIRENSCANNER

1 Virenscanner

Der Markt an Software für den Virenschutz ist groß. Neben den großen Platzhirschen wie Kaspersky, Norton oder Bitdefender gibt es eine Reihe weiterer Herstellern, die ebenfalls sehr effektive Produkte entwickeln. Teilweise werden Virenscanner sogar kostenlos angeboten und durch Werbung finanziert. Um den richtigen Scanner zu finden, sollten Sie bei kommerziellen Angeboten stets die Testversion in Anspruch nehmen. Diese können Sie in der Regel installieren und dann ohne Einschränkungen 30 Tage lang testen.

Um es vorwegzunehmen: Den besten Virenscanner, der uneingeschränkt empfehlenswert ist, gibt es nicht. Jede Software setzt andere Schwerpunkte bei der Abwägung zwischen hoher Sicherheit, einfacher Bedienbarkeit und guter Performance. Daher macht es Sinn, sich vorab einen Überblick über die Merkmale gängiger Antivirenprogramme zu informieren.

1.1 Scanengine

Die sogenannte Scanengine ist das Herzstück eines Virenscanners. Sie entscheidet darüber, welche Methoden die Software bei der Suche nach Viren und anderen Bedrohungen sowie bei der Problemlösung einsetzt. In den letzten Jahren sind die Scanengines der großen Hersteller immer ausgereifter und effektiver geworden. Allerdings rüsten natürlich auch die Entwickler von Viren auf und suchen nach Lücken in den bekannten Virenprogrammen.

1.1.1 Suche nach Bedrohungen

Eine der wichtigsten Funktionen eines Antivirenprogramms ist das Aufspüren von infizierten Dateien und anderen Bedrohungen auf dem Rechner. Denn Viren, die nicht gefunden werden, können logischerweise auch nicht unschädlich gemacht werden. Eine gute Scanengine verfügt also immer auch über eine sehr gute Erkennungsrate. Die Erkennungsrate der großen Hersteller erreicht mittlerweile knapp 100 Prozent aller bekannten Gefahren. Selbst die Hersteller, die ihre Produkte kostenlos anbieten, müssen sich was die Erkennungsleistung angeht in der Regel nicht hinter den kommerziellen Programmen verstecken.

1.1.2 Was sind Signaturen?

Eine gute Scanengine ist auf aussagekräftige Signaturen angewiesen. Im Prinzip handelt es sich dabei um die digitalen Fingerabdrücke von Viren. Bekannte Viren und andere Schadprogramme werden analysiert und deren Verhalten in einer Signatur umschrieben. Nun analysiert der Virenscanner die Daten auf dem Computer und gleicht diese mit den Signaturen ab. Werden Übereinstimmungen gefunden, wird die Datei als potenziell gefährlich eingestuft und der Nutzer erhält eine Warnung und Lösungsvorschläge. Die Verwendung von Signaturen hat den Vorteil, dass auch Viren gefunden werden können, die leicht verändert wurden aber dennoch eine ähnliche Signatur haben. Die Analyse von

Dateien und der Abgleich mit Signaturen ist ein sehr rechenintensiver Prozess. Je besser die Scanengine ist, desto besser fällt der Kompromiss aus Erkennungsleistung und Systemauslastung aus.

1.2 Regelmäßige Updates

Die meisten Virenscanner arbeiten mit Signaturen und Datenbanken, in denen Informationen zu allen bereits bekannten Bedrohungen gesammelt werden. Dementsprechend kann ein effektiver Virenschutz nur dann garantiert werden, wenn diese Signaturen und Datenbanken ständig aktuell gehalten werden. Deshalb versorgen die Hersteller ihre Antivirenprogramme mit regelmäßigen Updates, die in vielen Fällen stündlich, mindestens aber täglich stattfinden sollten. Denn jeden Tag tauchen im Internet neue bisher unbekannte Viren auf.

1.2.1 Automatische Updates aktivieren

Die meisten Virenscanner führen diese Updates automatisch aus, ohne dass der Nutzer tätig werden muss. Zwar besteht in der Regel die Möglichkeit, den Updatevorgang nur manuell zu starten, hiervon ist allerdings dringend abzuraten. Denn bereits um wenige Tage veraltete Datenbanken und Signaturen können ein deutliches Sicherheitsrisiko darstellen und dem Virenschutz im Wege stehen.

1.2.2 Neue Programmversionen

Die Updates der Datenbanken und Signaturen sind von den Programmupdates zu unterscheiden, die den Virenscanner auf eine neue Version erhöhen. Normalerweise werden kommerzielle Virenscanner nicht zu einem Festpreis verkauft, sondern für eine Jahresgebühr. Diese jährliche Zahlung umfasst dann die Nutzung der aktuellen Version sowie der neuen Versionen der Virensoftware. Die meisten Hersteller veröffentlichen einmal im Jahr eine neue Version der Software, die in der Regel die aktuelle Jahreszahl im Namen trägt. Diese neuen Versionen bringen meist Veränderungen in der Engine oder Funktionsweise der Software sowie zusätzliche Funktionen mit sich.

1.3 Heuristik

Die Heuristik ist eine mathematisch-analytische Methode, die von vielen Antivirenprogrammen zusätzlich zu Signaturen verwendet wird, um Viren aufzuspüren. Im Unterschied zu Signaturen werden Viren dabei nicht eindeutig identifiziert, sondern das Verhalten oder der Aufbau einer Datei analysiert. Dateien werden dann als gefährlich eingestuft, wenn ihr Verhalten dem eines Virus entspricht.

1.3.1 Vorteile der Heuristik

Die Verbreitung neuer Viren und Bedrohungen im Internet nimmt täglich zu. Die großen Hersteller der Virenscanner beschäftigen mittlerweile ganze Büros von IT-Spezialisten, die nichts anderes tun, als das Internet nach neuen Gefahren zu durchsuchen und die Signaturen entsprechend anzupassen. Dennoch hat der Virenschutz in diesem Wettlauf gegen die Kriminellen nicht immer die Nase vorne. Bereits ein kurzer Zeitraum zwischen Auftauchen einer Bedrohung und Update der Signaturen kann ausreichen, um den Rechner zu infizieren. Die Heuristik erlaubt es den Virenscannern jedoch, selbst unbekannte Bedrohungen zu finden. Und zwar ohne ein notwendiges Update. Grundsätzlich ist eine gut umgesetzt Heuristik deshalb ein deutlicher Sicherheitsgewinn.

1.3.2 Nachteile der Heuristik

Natürlich analysieren nicht nur die Hersteller von Antivirenprogrammen die neuen Viren und Schadprogramme. Auch deren Entwickler beobachten ganz genau, wie die Virenscanner arbeiten und passen ihre Viren entsprechend an. In der Regel werden zumindest ambitionierte Hacker und Kriminelle ihre Schadprogramme mit den gängigen Virenscannern testen. Erst wenn sie diesen Test bestehen, also auch von der Heuristik nicht erkannt werden, setzen die Programmierer ihre Viren frei. Deshalb stellt die Heuristik zwar eine wichtige Zusatzfunktion eines Virenscanners dar, absolute Sicherheit garantiert sie jedoch nicht.

1.4 Wenig Arbeitsspeicherbelastung

Je fortschrittlicher und komplizierter Viren werden, desto schwerer fällt es auch den Virenscannern, diese aufzuspüren. Für diese Aufgabe werden immer komplexere Algorithmen und Techniken notwendig, die selbst gut ausgerüstete Computer spürbar belasten können. Vor allem der Komplettscan von ganzen Festplatten kann bei immer größer werdenden Speicherkapazitäten durchaus mehrere Stunden in Anspruch nehmen. Auch das Öffnen und Bearbeiten von Dateien kann deutlich verlangsamt werden, wenn der Virenschutz im Hintergrund dauernd nach Bedrohungen sucht.

1.4.1 Lösungen der Hersteller

Natürlich kennen auch die Hersteller der Antivirenprogramme dieses Problem. Deshalb integrieren sie in der Regel Funktionen, mit denen der Nutzer gar nicht mehr mitbekommt, wenn ein Virenscan läuft. Beispielsweise werden systembelastende Scans ausgesetzt und später fortgeführt, wenn die Rechnerauslastung durch andere Anwendungen steigt. Oft werden auch gezielt Gamer mit sogenannten Gamefunktionen angesprochen, die beim Öffnen eines Spiels die Verlangsamung des Systems durch den Virenscanner verhindern.

1.4.2 Virenschutz richtig timen

Auch der Nutzer selbst kann beim Problem der Arbeitsspeicherbelastung nachhelfen. Die meisten Virenscanner bieten ihren Nutzern die Möglichkeit, feste Zeiten für Virenscans einzurichten. So kann die arbeitsintensive Arbeit der Antivirenprogramme auf Zeiten gelegt werden, in denen der Computer ohnehin nicht benötigt wird, also beispielsweise nachts oder in der Mittagspause.

1.5 Entfernen und reparieren beschädigter Dateien

Antivirenprogramme beschränken sich in der Regel nicht auf das bloße Aufspüren von Bedrohungen auf dem Computer. Zwar gibt es einige Programme, die tatsächlich nur nach Viren suchen und diese identifizieren. Solche Programme sind für Privatanwender jedoch in der Regel nutzlos und richten sich eher an professionelle Softwareanalytiker oder Systemadministratoren. Für private Nutzer ist die Reparaturleistung von entscheidender Bedeutung. Sie sorgt dafür, dass erkannte Probleme auch gelöst werden und der Computer wieder sicher wird und stellt gemeinsam mit der Erkennungsrate eines der größten Qualitätsmerkmale der Antivirenprogramme dar. Grundsätzlich wird der Nutzer beim Auffinden einer Bedrohung gefragt, ob er die Datei reparieren, in Quarantäne verschieben oder löschen will.

1.5.1 Infizierte Dateien reparieren

Die Reparatur einer infizierten Datei stellt die ideale Problemlösung dar. Denn sie ermöglicht nicht nur die Wiederherstellung der Computersicherheit, sondern auch die weitere Nutzung der infizierten Datei. Während die bekannten Virenscanner im Bereich der Erkennungsrate in der Regel sehr nah beieinander liegen, bestehen teilweise erhebliche Unterschiede bei der Reparaturmöglichkeit beschädigter Dateien.

1.5.2 Quarantäne und löschen

Kann eine infizierte Datei nicht repariert werden, hat der Nutzer die Möglichkeit, sie in die Quarantäne zu verschieben oder zu löschen. Die Quarantäne sorgt dafür, dass die Datei vom Rest des Systems isoliert wird und keinen Schaden mehr auf dem Computer anrichten kann. Quarantäne empfiehlt sich insbesondere dann, wenn Dateien infiziert wurden, die möglicherweise für das System relevant sind. Bevor Sie diese Dateien löschen, sollten Sie sie zunächst in die Quarantäne verschieben und überprüfen, ob das System weiterhin problemlos läuft. Das Löschen einer infizierten Datei stellt letztendlich die Notlösung dar, denn diese Datei können Sie anschließend nicht mehr nutzen. Um zu verhindern, dass wichtige persönliche Dateien infiziert werden und nicht mehr repariert werden können, sind regelmäßige Backups unbedingt zu empfehlen.

1.6 Sandbox

Vor allem die kommerziellen Antivirenprogramme bieten oft eine sogenannte Sandbox an. Diese ermöglicht es dem Nutzer, potenziell gefährliche Situationen und Aktionen in einer virtuellen Umgebung durchzuführen, die vom eigentlichen System völlig unabhängig ist. Der Vorteil besteht darin, dass selbst schlimmste Infektionen, die zur Beschädigung des ganzen Computers führen können, nicht mehr das eigentliche Arbeitssystem angreifen können. Dadurch wird bei solchen schwerwiegenden Infektionen die Neuinstallation des gesamten Betriebssystems unnötig.

Die Verwendung der Sandbox empfiehlt sich vor allem bei potenziell gefährlichen Dateien. Wenn Sie beispielsweise einen E-Mail-Anhang öffnen wollen, ohne sicher zu sein, dass die Quelle vertrauenswürdig ist, sollten Sie sicherheitshalber eine Sandbox verwenden. Auch der Download von fremden Dateien aus dem Internet ist in einer Sandbox wesentlich sicherer.

1.7 Schutz vor Phishing und Spam

Neben Viren gehört vor allem das Phishing zu den größten Bedrohungen für Internetnutzer. Insbesondere wenn Sie Funktionen wie Online Banking im Internet nutzen, sollten Sie Ihre Daten gut schützen, ansonsten könnten Sie leicht zum Opfer einer Phishing Attacke werden, bei der sich unbefugte Zugriff auf Ihre Daten verschaffen. Die Maschen der Kriminellen werden dabei immer ausgefeilter und sind längst nicht mehr so leicht zu durchschauen wie noch vor einigen Jahren. Beispielsweise imitieren Betrüger den Webauftritt von Banken und anderen Unternehmen mittlerweile so überzeugend, dass Sie mit dem bloßen Auge keinen Unterschied mehr feststellen können.

1.7.1 Auf Zertifikate achten

Um die Risiken des Phishings zu reduzieren, verfügen die Webseiten von Banken und großen Firmen über Sicherheitszertifikate, die vom Browser überprüft werden. Ihre Daten sollten Sie nur dann auf der Seite eingeben, wenn das Zertifikat gültig ist. Die kommerziellen Antivirenprogramme verstärken den bereits durch die Browser gegebenen Schutz zusätzlich und können viel schneller und vor allem aktueller auf neue Phishing Attacken reagieren.

1.7.2 Keylogger und Spam

Eine weitere große Gefahr beim Online Banking stellen sogenannte Keylogger dar, die Tastatureingaben speichern und an Unbefugte weiterleiten können. Dadurch können zum Beispiel Ihre Login Daten bei Ihrer Hausbank schnell in die falschen Hände geraten. Um sich vor dieser Bedrohung zu schützen, sollten Sie einen Virenscanner mit einer sogenannten virtuellen Tastatur wählen. Diese wird auf dem Bildschirm eingeblendet und über die Maus bedient. Dadurch sind Ihre Eingaben auf der Webseite der Bank stets sicher. Schließlich bieten viele Antivirenprogramme auch einen sehr effektiven Spamschutz, der meist als Plugin in Ihren E-Mail-Client integriert wird.

1.8 Intuitive Bedienung und Benutzeroberfläche

Die Funktionsweise von Antivirenprogrammen ist aufgrund der immer komplexer werdenden Bedrohungen ebenfalls immer komplizierter geworden. Was im Hintergrund während einem Virenscan geschieht, kann von den meisten Nutzern nicht nachvollzogen werden. Diesen kommt es in der Regel ohnehin nur auf einen möglichst effektiven Schutz an, egal wie dieser erreicht wird. Deshalb spielt die Gestaltung der Benutzeroberfläche eine entscheidende Rolle für die Qualität des Virenscanners. Je einfacher und selbsterklärender dem Nutzer die komplizierten Funktionen erläutert werden, desto besser.

1.8.1 Sicherheitsstufen

Grundsätzlich kann die Funktionsweise einer Scanengine durch die Veränderung von wesentlichen Parametern angepasst werden. So kann ein individuell optimaler Ausgleich zwischen Sicherheit und Systemauslastung erreicht werden. Je sicherer die Engine arbeitet, desto mehr Leistung benötigt sie in der Regel und umgekehrt. Anstatt nun aber die Parameter der Engine einzeln zu ändern, können die Nutzer die Leistung der Engine in der Regel über Sicherheitsstufen von schwach bis sehr hoch einstellen. Viele Hersteller ermöglichen auch die Anpassung der Engine anhand der Hardwareausstattung des Rechners.

1.8.2 Benutzeroberfläche

Neben den verschiedenen Anpassungsmöglichkeiten sollte die Benutzeroberfläche aufgeräumt und übersichtlich wirken. Die wichtigsten Funktionen müssen sich mit wenigen Klicks erreichen lassen, ohne lange in Menüs herumsuchen zu müssen. Auch die Zusatzfunktionen wie Firewall oder Timer für den Komplettscan sollten durch aussagekräftige Symbole repräsentiert werden. Je intuitiver die Benutzeroberfläche ist, desto leichter wird es Ihnen fallen, das Potenzial des Antivirenprogramms voll auszuschöpfen.

2 Diese Gefahren lauern im Internet

Von Computerviren dürfte jeder Internetnutzer schon einmal gehört haben. Auch Trojaner dürften zumindest vom Namen her bekannt sein. Neben diesen offensichtlichen Bedrohungen gibt es jedoch noch eine Reihe von weiteren Gefahren, deren Existenz den meisten Menschen im Internet nicht bewusst ist. Beispielsweise meldet die Polizei jährlich Tausende von Phishing-Opfern, die auf teilweise sehr dreiste Maschen hereinfallen und dabei oft einen finanziellen Schaden erleiden. Auch die alltägliche Gefahr durch Hacker und Spyware wird oft leichtfertig unterschätzt.

2.1 Daten richtig schützen

Neben dem definitiv gegebenen finanziellen Risiken eines Computerangriffs spielt noch der Schutz der Privatsphäre eine wichtige Rolle. Seltsamerweise gehen viele Menschen im Internet viel leichtsinniger mit persönlichen Daten um wie im normalen Leben. Schließlich würden Sie einer fremden Person, die Sie auf der Straße anspricht und nach Anschrift, Telefonnummer, E-Mail und Bankverbindung fragt, auch nicht Auskunft erteilen. Genau diese Daten sind ohne den entsprechenden Schutz im Internet aber mit relativ geringem Aufwand für fremde Personen erhältlich. Umso wichtiger ist es deshalb, diese Daten mit einem guten und effektiven Antivirenprogramm zu schützen. Darüber hinaus sollten Sie sich mit den wichtigsten Gefahren im Internet auseinandersetzen und lernen, wie Sie diese vermeiden können.

2.2 Viren

Von Computerviren hat wohl jeder Mensch schon einmal gehört, der das Internet auch nur gelegentlich nutzt. Im Prinzip sind Viren Computerprogramme, die fremde Computersysteme infizieren und sich von dort aus selbstständig weiter verbreiten. Ihren Namen haben Computerviren also von ihrer Funktionsweise, die ihren Namensvettern in der Natur ähnelt.

2.2.1 Harmlos bis gefährlich

Die ersten Computerviren wurden in den 1980er Jahren entwickelt und sind mittlerweile wesentlich komplexer und auch potenziell gefährlicher geworden. Teilweise sind die Viren harmlos und beschränken sich auf die Weiterverbreitung, ohne Schaden anzurichten. Diese Viren werden von den Programmierern meist aus purem Ehrgeiz entwickelt und sollen deren Fähigkeiten demonstrieren. Andere Viren können den Rechner völlig lahmlegen, wichtige Daten löschen oder sensible und private Informationen stehlen. Der Schutz vor Viren ist deshalb auch der Hauptanwendungsbereich von Virenscannern.

2.2.2 Unbekannte Quellen meiden

Besonders häufig sind Infektionen mit Computerviren aus unbekannten oder illegalen Quellen. In den letzten Jahren hat sich vor allem das Filesharing als Nährboden für Computerviren präsentiert. Sehr oft infizieren aber auch unbedarfte Gelegenheitssurfer ihren Computer mit einem Virus, indem sie zum Beispiel einen E-Mail-Anhang aus einer unbekannten Quelle öffnen.

2.3 Trojaner & Spyware

Im Gegensatz zum Computervirus gelangt ein sogenannter Trojaner, auch Spyware genannt, nicht unbemerkt auf den Rechner des Opfers. Tatsächlich lädt sich der Computernutzer den

Trojaner bewusst auf das System, weil er ihn für ein nützliches Programm hält. Oft sind Trojaner auch in Mediendateien wie Filmen oder MP3s versteckt. Wird die entsprechende Datei ausgeführt, führt der Trojaner im Hintergrund eine sogenannte Routine aus, die meist in der Ausspähung von Daten besteht und für den betroffenen Nutzer schlimme Konsequenzen haben kann. Im Prinzip handelt es sich bei Trojanern also um das digitale Pendant des trojanischen Pferdes aus der griechischen Mythologie.

Ohne einen vernünftigen Virenschutz ist es fast unmöglich, einen Trojaner zu erkennen oder zu entfernen. Darin liegt auch die große Gefahr. Oft arbeiten Trojaner jahrelang auf einem ungeschützten System und stehlen kontinuierlich Daten. Prinzipiell kann es sich dabei um sämtliche privaten Informationen handeln, auf die auch der Computer Zugriff hat. Dazu gehören natürlich auch Daten von Kreditkarten, Bankkonten, Geschäftsunterlagen und persönliche Daten wie Urlaubsfotos. Im Internet hat sich mittlerweile ein großer Schwarzmarkt entwickelt, der mit solchen Daten handelt. Bis der unbemerkte Datenklau dann in einen finanziellen oder persönlichen Schaden umschlägt, ist es nur noch eine Frage der Zeit.

2.4 Malware

Malware ist der Oberbegriff für sämtliche Schadprogramme, die vom Benutzer unbemerkt Schaden auf dessen Computer anrichten. Hierzu gehören insbesondere auch Computerviren und Trojaner. Malware wird häufig durch kostenlose Software aus fragwürdigen Quellen verbreitet, aber auch einzelne Computerdateien wie Bilder, Audiodateien oder Videos können Malware erhalten.

2.4.1 Arten von Malware

Die zwei häufigsten und bekanntesten Fälle von Malware sind Viren und Trojaner. Während Viren vor allem über ihre selbstständige Weiterverbreitung definiert werden, wurden Trojaner hauptsächlich auf die unbemerkte Ausführung schädlicher Aktionen im Hintergrund optimiert. Darüber hinaus haben sich vor allem in den letzten Jahren noch weitere Unterarten der Malware herausgebildet, zu denen allem die sogenannte Ransomware gehört. Dabei werden wichtige Dateien auf dem Computer gesperrt und der Nutzer wird zur Zahlung eines Lösegeldes, oder auf Englisch ransom, aufgefordert. Ein weniger dramatischer aber ebenfalls ärgerlicher Fall von Malware ist die sogenannte Scareware. Dabei erhält der Nutzer durch gefälschte Virenmeldungen den Eindruck, sein Rechner sei infiziert und bekommt ein meist kostenpflichtiges, in Wahrheit aber unnützes Programm zur Lösung des Problems angeboten.

2.4.2 Schutz vor Malware

Die verschiedenen Varianten von Malware, zu denen in fast monatlichen Abständen neue Bedrohungen hinzukommen, veranschaulichen die zahlreichen Gefahren im Internet. Gute

Antivirenprogramme erkennen neben den klassischen Viren in der Regel auch andere Arten von Malware und vermitteln einen effektiven Schutz vor diesen Gefahren. Vernünftige Lösungen zum Virenschutz werden von vielen Herstellern mittlerweile auch kostenlos angeboten.

2.5 Adware

Unter dem Begriff Adware versteht man Software, die meist kostenlos angeboten und im Gegenzug durch Werbeeinblendungen finanziert wird. Diese Einblendungen können entweder in der Software selbst oder in anderen Bereichen des Systems, etwa im Webbrowser stattfinden. Solange der Nutzer bei der Installation über diese Werbemethode informiert wird, ist gegen Adware grundsätzlich nichts einzuwenden. Allerdings gibt es heute viele Fälle von Adware, die ganz klar der Malware zuzurechnen sind und zwar nicht so gefährlich sind wie andere Viren, dafür aber sehr unangenehm und lästig sein können.

2.5.1 Unerwünschte Werbung

Adware ist dann dem Bereich der Computerschädlinge zuzurechnen, wenn der Nutzer nicht nach seinem Einverständnis für die Werbung gefragt wird. Außerdem installieren viele schädliche Adwareprogramme ihre Werbung so tief in das System, dass sie nur noch schwer zu entfernen sind. Oft betrifft Adware den Webbrowser. Dabei wird zum Beispiel die integrierte Suchmaschine oder die Startseite geändert. Teilweise werden auch die Texte der besuchten Webseiten nach werberelevanten Keywords gescannt und entsprechende Links direkt in den Text eingefügt. Adware kann für den Nutzer sehr nervig sein und die Leistungsfähigkeit des Systems erheblich verschlechtern.

2.5.2 Schutz vor Adware

Ein wirksamer Schutz vor Adware besteht bereits darin, kostenlose Software nur aus vertrauenswürdigen Quellen zu installieren und während der Installation die entsprechenden Hinweise genau zu lesen. In der Regel ist die Installation von legaler Adware freiwillig und kann bei der Installation untersagt werden. Antivirenprogramme der großen Hersteller beinhalten oft auch einen effektiven Schutz vor Adware, kostenlose Virenscanner bieten diesen Schutz in der Regel nicht.

2.6 Hacker

Der Begriff Hacker ist im allgemeinen Sprachgebrauch eher negativ besetzt und wird oft für Kriminelle verwendet, die in fremde Systeme eindringen und dabei Schaden anrichten. Tatsächlich ist die Hackerszene jedoch viel differenzierter. Insbesondere führt nicht jeder Hacker Böses im Schilde. Stattdessen handelt es sich bei Hackern um Technikenthusiasten, denen die Analyse von Systemen Spaß machen und die sich zur entsprechenden Szene zählen.

2.6.1 Gefahren durch Hacker

Auch wenn die wirklich gefährlichen Hacker nur einen Bruchteil der Szene darstellen, geht von ihnen doch eine beträchtliche Gefahr für Internetnutzer aus. Denn einige Hacker nutzen ihre Fähigkeiten, um sich selbst zu bereichern, indem sie in fremde Computersysteme eindringen, dort Schaden anrichten oder Dateien stehlen, die später missbraucht oder weiterverkauft werden. Verschärft wird die Gefahr dadurch, dass viele Techniken der Hacker im Internet mittlerweile mit wenig Aufwand erlernt werden können. So genügt heute bereits etwas kriminelle Energie, um auch ohne besondere Kenntnisse oder Fertigkeiten Schaden auf fremden Computern anrichten zu können.

2.6.2 Hacker abwehren

Hacker befinden sich im ständigen Wettlauf mit den Anbietern von Sicherheitsprogrammen. Ein absolut lückenloser und unbezwingbarer Schutz ist auch mit einem kostenpflichtigen und professionellen Antivirenprogramm nicht zu erreichen. Dennoch sollten Sie es den Hackern nicht zu leicht machen. Denn völlig ungeschützte Computer laden kriminelle Hacker geradezu zum Angriff ein.

2.7 Phishing und Keylogger

Phishing ist eine relativ neue Gefahr im Internet, die vor allem Kunden von Onlinebanking oder Internetshops betrifft. Im Prinzip handelt es sich dabei um einen klassischen Betrug mit den modernen Methoden des Internets. Häufig läuft die Masche so ab, dass das Opfer eine E-Mail oder eine Nachricht bekommt, in der sich der Täter als vertrauenswürdige Quelle, etwa die Hausbank oder einen Onlineshop, ausgibt. Das Opfer wird nun zur Preisgabe von Informationen wie Passwort oder Zahlungsdaten aufgefordert. Tatsächlich landen die Daten jedoch nicht bei der vertrauenswürdigen Stelle, sondern bei Kriminellen. Diese können sich nun gegenüber der Bank oder dem Shop als das Opfer ausgeben und Geld abheben oder Waren bestellen.

2.7.1 Phishing durch Trojaner

Noch perfider ist die Methode, in der die Daten des Opfers durch einen Trojaner abgefangen werden, ohne dass das Opfer etwas davon mitbekommt. Teilweise handelt es sich dabei um sogenannte Keylogger, die sämtliche Tastatureingaben des Opfers aufzeichnen und weiterleiten. So gelangen die Kriminellen an Passwörter und andere persönliche Daten.

2.7.2 Schutz vor Phishing

Um sich wirkungsvoll vor Phishing Attacken zu schützen, sollten Internetnutzer ihre Passwörter und vertraulichen Informationen niemals per E-Mail oder auf Webseiten ohne sichere Verbindung preisgeben. Eine sichere Verbindung kann durch den https-Anfang einer URL und die Einblendung eines entsprechenden Zertifikats erkannt werden. Vor Trojanern und Keyloggern können nur Antivirenprogramme wirksam schützen.

2.8 Spam

Spam dürfte wohl jeder Internetnutzer kennen, der über eine eigene E-Mail-Adresse verfügt. Im Prinzip handelt es sich dabei um unerwünschte E-Mails. Zu Beginn der Internetzeitalters bestand Spam aus nervigen aber harmlosen Werbenachrichten im E-Mail-Postfach. Mittlerweile ist aus Spam jedoch eine echte Bedrohung geworden, denn viele Internetkriminelle nutzen Spam etwa für Phishing Attacken und geben sich als Hausbank des Opfers aus. Häufig enthalten Spam-Emails auch Dateianhänge, die Viren und andere Schädlinge auf den Rechner schleusen. Es gibt also gute Gründe, sich effektiv vor Spam zu schützen.

Der Schutz vor Spam ist nicht nur eine Sicherheitsfrage, sondern trägt auch zur Steigerung der Produktivität in Unternehmen bei, immerhin geht durch die Aussortierung von Spamnachrichten viel Arbeitszeit verloren. Die Antivirenprogramme der großen Hersteller bieten in der Regel sehr effektive Funktionen zum Schutz vor Spam, diese Spamfilter sind jedoch häufig schon in E-Mail-Clients integriert. Nutzer können sich darüber hinaus schützen, indem sie ihre E-Mail-Adresse nicht im Klartext auf Webseiten veröffentlichen. Mittlerweile gibt es Programme, die das Internet nach öffentlichen E-Mail-Adressen durchsuchen und diese Adressen dann mit Spam überfluten. Stattdessen sollten Sie etwa eine Grafik nutzen, die ihre E-Mail-Adresse enthält oder das @-Symbol beispielsweise durch at oder ät verfremden.

3 Wie funktioniert ein Virenscanner?

Antivirenprogramme haben die Funktion, den Rechner und andere Geräte wie Smartphones oder Tablets vor schädlichen Programmen zu schützen. Mittlerweile gibt es mehrere Prinzipien, nach denen diese Programme arbeiten. Dabei stehen die Entwickler der Virenscanner im ständigen Wettlauf mit Hackern und anderen Computerkriminellen. Deshalb verlassen sich moderne Antivirenprogramme häufig nicht nur auf eine einzige Technik zum Virenschutz, sondern setzen auf mehrere Funktionsweisen gleichzeitig.

3.1 Aktualität ist wichtig

Unabhängig davon, welche Technik im Antivirenprogramm zum Einsatz kommt, ist die Aktualität der Software von entscheidender Bedeutung für einen effektiven Virenschutz. Fast täglich werden im Internet neue Viren und Bedrohungen entdeckt, deshalb stellen die großen Anbieter der Antivirenprogramme auch regelmäßige Updates zur Verfügung. Zwischen dem Bekanntwerden einer Bedrohung und einem Update liegen oft nur wenige Minuten. Die Nutzer der Virenscanner sollten deshalb darauf achten, ihre Software

möglichst aktuell zu halten. Hierfür gibt es in den meisten Programmen eine Funktion für automatische Updates.

3.2 Echtzeitscanner

Viele Antivirenprogramme verfügen über Echtzeitscanner, die sich nach der Installation vor das Dateisystem des Systems schalten und bei jedem Zugriff auf eine Datei einen Scan der jeweiligen Datei durchführen. Hierbei muss zwischen dem Scan beim Lesevorgang sowie dem Scan beim Schreibvorgang unterschieden werden. Ein Lesevorgang liegt immer dann vor, wenn eine Datei auf dem Rechner geöffnet wird. Wird eine Date dagegen erstellt, gespeichert oder verändert, spricht man vom Schreibvorgang.

Das Problem bei Echtzeitscannern ist zum einen die hohe Belastung des Computers beim Öffnen oder Schreiben von Dateien, die zu erheblichen Geschwindigkeitseinbußen führen kann. Dies wird häufig dadurch umgangen, dass der Scan auf den Schreibvorgang beschränkt wird, der wesentlich seltener vorkommt als der Lesevorgang. Hierunter leidet jedoch wieder die Sicherheit. Denn eine mit einem Virus infizierte Datei, die vor der Installation des Virenschutzes gespeichert wurde, kann dann beim Öffnen nicht mehr erkannt werden. Echtzeitscanner sollten deshalb mit regelmäßigen manuellen Scans kombiniert werden.

3.3 Manueller Scanner

Manuelle Virenscanner sind mittlerweile in fast allen Antivirenprogrammen integriert. Der größte Unterschied zum Echtzeitscanner liegt darin, dass ein manueller Scanner nicht nur einzelne Dateien, sondern die gesamten Festplatten des Rechners nach Viren und Schadsoftware durchsucht. Werden infizierte Dateien gefunden, kann der Nutzer das weitere Vorgehen bestimmen und hat in der Regel die Wahl zwischen einer Reparatur der Datei, der Quarantäne oder dem Löschen. Diese Funktion ist genauso wichtig wie das eigentliche Auffinden der Viren, schließlich geht es dem Nutzer ja gerade darum, die Gefahr durch infizierte Dateien zu beenden.

Da Echtzeitscanner lückenlos das gesamte System durchsuchen, bieten sie grundsätzlich die größte Sicherheit vor Viren. Das setzt allerdings voraus, dass der manuelle Scan möglichst häufig und regelmäßig durchgeführt wird. Wegen der recht hohen Systemauslastung während dem Scan empfiehlt es sich, den Scan zu Zeiten durchzuführen, in denen der Computer nicht für andere leistungsintensive Aufgaben genutzt wird. Hierfür bieten die meisten Virenscanner eine Timerfunktion an, mit der der Nutzer die regelmäßigen Scans auf beliebige Zeitintervalle und Uhrzeiten legen kann. So können die Komplettscans beispielsweise jede Nacht oder jeden Tag in der Mittagspause durchgeführt werden.

3.4 Online Virenscanner

Neben den klassischen Virenscannern, die auf der Festplatte des Computers installiert werden, gibt es noch sogenannte Online-Virenscanner. Diese benötigen keine Installation, sondern werden über das Internet aufgerufen und können einzelne Dateien oder sogar ein gesamtes System scannen. Nicht zu verwechseln sind Online-Scanner jedoch mit fest installierten Virenscannern, die lediglich regelmäßige Updates aus dem Internet beziehen, während der eigentliche Scan lokal abläuft.

Sicherheitsexperten empfehlen den Einsatz von Online Scannern nur zum Erhalt einer zweiten Meinung. Findet der installierte Virenscanner etwa eine infizierte Datei, kann dieses Ergebnis mit einem Onlinescanner überprüft werden. Im Vergleich zu Echtzeitscannern und insbesondere manuellen Komplettscannern bieten die Onlinescanner jedoch keinen ausreichenden Virenschutz. Insbesondere werden Virusinfektionen nicht präventiv verhindert, sondern lassen sich nur im Nachhinein erkennen und beheben.

3.5 Sonstige Scanner

Neben Echtzeitscannern, Online-Scannern und manuellen Scannern gibt es noch weitere Virenscanner, die vor allem von Unternehmen und Providern im Internet eingesetzt werden. Oft besteht ihre Aufgabe in der Überwachung der Netzwerkverbindungen, Viren und Bedrohungen werden also bereits aufgespürt und abgewehrt, bevor sie überhaupt in Kontakt mit einem einzelnen Rechner geraten. Ebenfalls sehr effektiv sind sogenannte Proxyscanner.

Ein Proxyscanner schaltet sich direkt in die Verbindung zwischen zwei Computern und fungiert quasi als Torwächter. Wird eine Datei von einem Server angefordert, wird diese zunächst an den Proxy geleitet, überprüft und bei einem Virenbefall entweder repariert oder gelöscht. Nur saubere Dateien werden dann an den Zielrechner weitergeleitet. Diese Technik wird vor allem von E-Mail-Providern verwendet. Hierbei werden E-Mails bereits auf dem Mailserver gescannt, bevor sie an das Postfach des Empfängers weitergeleitet werden.

4 Überblick über die wichtigsten Virenscanner

Auf dem Markt für Virenschutz gibt es viele Produkte, die für einen einmaligen Kaufpreis, eine Jahresgebühr oder sogar kostenlos erhältlich sind. Vor allem die kommerziellen Angebote warten dabei in der Regel mit einer Vielzahl von Zusatzfunktionen und Extras auf. Preislich liegen die Produkte für Privatanwender alle nahe beieinander, auch bei der Erkennungsrate und der Reparaturleistung, den beiden wichtigsten Qualitätsmerkmalen für ein Antivirenprogramm, fällt keiner der Anbieter deutlich hinter die Konkurrenz zurück.

4.1 Die Qual der Wahl

Letztendlich kommt es deshalb darauf an, welche Funktionen Sie von Antivirenprogrammen erwarten oder dringend brauchen. Sind Sie beispielsweise beruflich auf das Internet angewiesen und nutzen oft Online-Banking, sollten Sie bei Ihrer Wahl darauf achten, dass das Produkt entsprechende Zusatzfunktionen bietet. Kommt es Ihnen dagegen darauf an, dass Sie während Computerspielen nicht durch den Start einer kompletten Systemprüfung gestört werden, sollte die Auslastung des Arbeitsspeichers ein Entscheidungskriterium für Sie sein. Letztendlich erhalten Sie aber bei allen Anbietern einen zuverlässigen und effektiven Virenschutz.

4.2 AVG

Die tschechische Firma AVG vertreibt mehrere Produkte, mit denen Privatanwender einen umfassenden Virenschutz erreichen können. Mit Investoren wie Intel und Microsoft ist AVG einer der finanzkräftigsten Anbieter auf dem Markt. Die wesentlichen Antivirenprogramme werden kostenpflichtig angeboten, allerdings existiert auch eine kostenlose Version namens AVG Anti-Virus Free. Allerdings bietet diese Version nur Schutz vor den rudimentärsten Gefahren im Internet und ist für Vielsurfer deshalb nur bedingt geeignet.

4.2.1 AVG Anti-Virus

Das erfolgreichste Produkt des Herstellers ist das Virenprogramm AVG Anti-Virus. Es verfügt neben einem klassischen Virenscanner mit aktuellen Signaturen und leistungsfähiger Heuristik auch über einen sogenannten Link-Scanner. Dieser überprüft sämtliche von einer Webseite abgehenden Links auf ihre Sicherheit, noch bevor der Nutzer darauf geklickt hat.

4.2.2 AVG Internet Security

Die AVG Internet Security Suite ergänzt die Funktionen von Anti-Virus um eine Firewall, die sämtliche Verbindungen des Computers mit dem Internet absichert. Der Nutzer kann festlegen, welche Programme unbeschränkten Zugang zum Internet erhalten sollen, und welche Anwendungen erst um eine Erlaubnis fragen müssen.

4.3 Bitdefender

Bitdefender gehört seit dem Start 2007 zu den bekanntesten und erfolgreichsten Antivirenprogrammen auf dem Markt. Verantwortlich die Entwicklung ist ein Team in Rumänien. Seinen Erfolg verdankt Bitdefender vor allem den innovativen und leistungsfähigen Zusatzfunktionen, die den eigentlichen Virenschutz ergänzen.

4.3.1 Starke Heuristik

Die in Bitdefender integrierte Heuristik namens B-Have gehört zu den leistungsfähigsten Heuristik-Funktionen auf dem Markt. Neue Dateien werden im Hintergrund in einer

virtuellen und sicheren Umgebung geöffnet und deren Verhalten analysiert. Entspricht das Verhalten einem Computervirus, erhält der Nutzer eine Warnung. B-Have ist damit ein recht zuverlässiges System zum Aufspürung von bisher unbekannten Bedrohungen.

4.3.2 Intelligenter Spamschutz

Darüber hinaus bietet Bitdefender neben den Antivirenfunktionen auch einen Spamschutz, der erkannte Spammails analysiert und nach ähnlichen Nachrichten sucht. Dadurch lernt der Spamfilter von Bitdefender ständig dazu und führt nach einigen Tagen oder Wochen der Nutzung zu sehr zuverlässigen Ergebnissen beim Filtern von Spammails. Der Spamschutz von Bitdefender ist mit den meisten gängigen Mailclients kompatibel.

4.4 Eset

Eset ist ein Virenprogramm aus der Slowakei, das sich vor allem in der E-Sport-Szene großer Beliebtheit erfreut. Das liegt zum einen daran, dass Eset als Sponsor von Events aus dem E-Sport-Bereich auftritt, allerdings dürfte auch die im Vergleich zur Konkurrenz sehr geringe Systembelastung ein Grund für den Erfolg unter Gamern sein.

4.4.1 Lange Tradition

Bereits 1998 entwickelte Eset ein Virenprogramm namens NOD, das auf MS-DOS lief. Eine Windows Version erschien wenig später, heute sind die Produkte der Firma für Windows, Linux, BSD und Solaris erhältlich. Das erfolgreichste Produkt ist das Virenprogramm ESET Antivirus. Es zeichnet sich durch eine besonders geringe Belastung des Computers aus, ohne dabei deutlich hinter die Effektivität der Konkurrenzprodukte zu fallen.

4.4.2 Kostenlos im Internet

Seit einiger Zeit bietet Eset neben den kommerziellen Programmen auch einen Onlinescanner an, der den Computer ohne vorherige Installation nach Viren und anderen Schadprogrammen durchsucht. Dieser Onlinescanner sollte allerdings von Privatanwendern nicht als einziger Antivirenschutz genutzt werden, denn eine Funktion zum Reparieren der entsprechenden Dateien fehlt bei diesem Angebot.

4.5 F-Secure

F-Secure ist eine finnische Firma, die sich auf die Entwicklung von Virenschutzlösungen spezialisiert hat. Privatanwender haben die Wahl aus mehreren Produkten für unterschiedliche Betriebssysteme. So bietet F-Secure neben der Windowsversion nicht nur eine Version für Mac OSX, sondern auch für das mobile Smartphone-Betriebssystem Android an.

4.5.1 Die verschiedenen Versionen

Das erfolgreichste Virenprogramm von F-Secure ist F-Secure Antivirus, das sowohl Gelegenheitsnutzern als auch Vielsurfern einen ausreichenden Schutz vor Viren und anderen Schadprogrammen bietet. Dieser Schutz kann durch das Paket InternetSecurity um eine Firewall, effektiven Spamschutz und andere Funktionen erweitert werden.

4.5.2 Mobile Sicherheit

Wie viele andere Hersteller von Virenprogrammen ist auch F-Secure auf dem Markt für Virenprogramme für Smartphones vertreten und verteibt eine mobile Version seines Virenschutzes. F-Secure Mobile Security hält Android-Smartphones dabei nicht nur sicher vor Viren und Spyware, sondern bietet auch eine Anti-Diebstahlsfunktion, mit der das Handy nach einem Diebstahl lokalisiert und notfalls gesperrt oder gelöscht werden kann.

4.6 G-Data

G-Data ist das größte deutsche Softwareunternehmen für IT-Sicherheit und bereits seit den späten 80-er Jahren in diesem Bereich tätig. In Deutschland verdankt G-Data seine Marktführerposition vor allem sehr guten Ergebnissen in den Tests von Stiftung Warentest und anderen unabhängigen Einrichtungen. Seit 2013 bietet G-Data auch eine Mac-Version seines Virenschutzes an.

4.6.1 Übersichtliche Benutzeroberfläche

Große Stärke von G-Data ist neben der sehr guten Erkennungsrate und Reparaturleistung auch die übersichtliche Benutzeroberfläche, in der alle wichtigen Funktionen mit sehr wenigen Klicks erreichbar sind. Auch für Computerneulinge ist das Programm einfach zu bedienen. Beispielsweise kann der Nutzer auswählen, ob G-Data lieber schnell oder gründlich arbeiten soll, wobei für beide Möglichkeiten eine jeweils andere Scanengine zum Einsatz kommt.

4.6.2 Sicherheit für Smartphones

Neben den Produkten für PC und Mac vertreibt G-Data auch einen Virenschutz für Android Handys, der als App installiert wird und das Betriebssystem gegen Bedrohungen aus dem Internet absichert. Auch Online Banking wird durch die Zusatzfunktion Bank Guard deutlich sicherer.

4.7 Kaspersky

Der Name Kaspersky ist für die meisten Nutzer untrennbar mit dem Thema Virenschutz verbunden. Bereits seit den 80er Jahren entwickelt das russische Unternehmen Kaspersky Lab Programme zum Entdecken und Entfernen von schädlichen Programmen. Mittlerweile

bietet Kaspersky mit seinen Produkten für Privatanwender und Unternehmen die weltweit erfolgreichsten Virenscanner an.

4.7.1 Gute Engines

Die langjährige Erfahrung kommt Kaspersky vor allem bei der Entwicklung von Scanengines zugute. Viele Hersteller anderer Virenprogramme lizensieren mittlerweile die Engine von Kaspersky, anstatt Zeit und Geld in die Entwicklung eigener Engines zu investieren. Die Kaspersky Engine zeichnet sich dabei vor allem durch hohe Geschwindigkeit und eine sehr hohe Erkennungsquote aus.

4.7.2 Produkte für Privatanwender

Wie die meisten Anwender unterteilt auch Kaspersky seine Produktfamilie in die Bereiche Antivirus und Internet Security. Während Kaspersky Antivirus einen sehr effektiven Schutz vor Viren und Malware bietet, bringt Kaspersky Internet Security viele Zusatzfunktionen wie einen intelligenten Spamfilter, eine virtuelle Tatstatur für Online Banking oder eine Sandbox mit.

4.8 Microsoft Windows Defender

Microsoft Windows Defender ist ein Sicherheitsprogramm der amerikanischen Firma Microsoft. Ursprünglich wurde die Software für Windows Nutzer kostenlos zum Download angeboten. Seit Windows 8 ist Windows Defender ein fester Bestandteil von Windows. Im Gegensatz zu den meisten anderen Lösungen für den Virenschutz konzentriert sich Windows Defender nicht auf Computerviren, sondern auf Spyware und Malware.

4.8.1 Kostenloser Basisschutz

Der größte Vorteil für die Anwender besteht darin, dass Windows Defender für Nutzer des Microsoft Windows Betriebssystems kostenlos ist und einen durchaus zuverlässigen Schutz vor Spyware bietet. Zwar verfügt das Programm auch über rudimentäre Funktionen zum Aufspüren und Entfernen von Computerviren, einen vollwertigen Virenscanner kann und will Windows Defender jedoch nicht ersetzen.

4.8.2 Nur mit Internet Explorer

Das volle Potenzial entfaltet der Windows Defender nur im Zusammenspiel mit dem Browser Internet Explorer. Dort ist er fest in den Browser integriert und gibt dem Nutzer Kontrolle über die installierten AddOns und Zusatzfunktionen. Andere Browser wie Firefox oder Google Chrome werden derzeit jedoch nicht unterstützt.

4.9 Norton

Norton ist der Markenname von Antivirenprogrammen der amerikanischen Firma Symantec. Seinen größten Erfolg hatte der Virenschutz von Norton in den späten 90er Jahren, als er zu den Marktführern im Bereich der Internetsicherheit zählte. Mittlerweile haben die Norton Produkte etwas den Anschluss an die Konkurrenz verloren, machten aber jüngst durch sehr gute Ergebnisse in den einschlägigen Tests wieder auf sich aufmerksam.

4.9.1 Norton Antivirus

Norton Antivirus ist ein klassisches Antivirenprogramm, das Viren und Schadprogramme auf dem Rechner aufspürt und beseitigt. Dabei verlässt sich das Programm hauptsächlich auf die regelmäßigen Updates, für die der Nutzer ein einjähriges Abonnement kaufen muss. Während Norton stets auf sehr gute Werte bei Erkennungsquote und Reparaturleistung kam, wurden die hohe Speicherauslastung und die vergleichsweise geringe Arbeitsgeschwindigkeit von Nutzern und Testern kritisiert. Mittlerweile hat Norton in diesem Bereich jedoch deutlich nachgebessert.

4.9.2 Norton Internet Security

Die Sicherheitssuite Norton Internet Security enthält neben dem eigentlichen Virenprogramm Norton Antivirus noch eine Firewall, einen Spamfilter, Funktionen zum Schutz vor Phishing sowie vor Identitätsdiebstahl im Internet. Außerdem gehört zur Internet Security Suite auch ein Virenprogramm für mobile Endgeräte wie Smartphones und Tablets.

4.10 Sonstige Virenscanner

Bei der Suche nach einem geeigneten Virenprogramm werden Sie sich in erster Linie mit einem Vergleich der großen Anbieter beschäftigen. Dennoch gibt es neben den Marktführern noch eine Reihe von kleineren Entwicklern, die ebenfalls sehr effektiven Schutz bieten und ihre Produkte dabei oft deutlich günstiger oder sogar ganz kostenlos anbieten. In der Regel erhalten Sie bei diesen Antivirenprogrammen jedoch nicht die Fülle an sinnvollen Zusatzfunktionen wie Firewall, Sandbox oder mehreren Engines.

4.10.1 Tests lesen

Um sich einen Überblick über das Angebot von Virenscannern abseits der großen Hersteller zu machen, empfiehlt sich die regelmäßige Lektüre der Testberichte von Computermagazinen oder unabhängigen Testern für Virensoftware. Hier werden neben den großen Programmen in der Regel auch kleinere Hersteller berücksichtigt und fair getestet.

4.10.2 Innovative Ideen

Während andere, kleinere Virenprogramme zwar oft nicht den großen Funktionsumfang der Marktführer bieten können, setzen sie dafür oft auf neue und originelle Ideen. So integriert

sich das OpenSource Projekt ClamWin beispielsweise direkt in den Windows Explorer und setzt bei seiner Weiterentwicklung auf die Ideen und die Mitarbeit seiner Nutzer.

5 Kostenlose Virenscanner

Für die Virenprogramme der großen Hersteller wird in der Regel eine jährliche Gebühr fällig, die quasi als Abonnement für die Nutzung der Software und der regelmäßigen Updates von Datenbanken und Signaturen zu verstehen ist. Die Jahresgebühr ist dabei gemessen an der Gefahr, die ohne Virenschutz besteht, in der Regel durchaus angemessen, dennoch sind kostenlose Virenprogramme bei privaten Anwendern sehr beliebt.

5.1 Zusatzfunktionen gegen Aufpreis

Allerdings geht es auch den Anbietern von kostenlosem Virenschutz selbstverständlich darum, Geld mit ihren Produkten zu verdienen. Das geschieht teilweise mittels einer Finanzierung durch Werbeeinblendungen, oft sind die kostenlosen Virenscanner in ihrem Funktionsumfang jedoch deutlich eingeschränkt und sollen die Anwender zum Kauf der unbeschränkten, kostenpflichtigen Version animieren.

5.2 Können kostenlose Virenscanner mithalten?

In den Tests der einschlägigen Labors und Computermagazine werden kostenlose Virenprogramme regelmäßig mit den kostenpflichtigen Produkten vergleichen. Dabei zeigt sich häufig ein messbarer Unterschied in den Bereichen Erkennungsquote, Reparaturleistung und Systembelastung. Allerdings dürfte der durch die kostenlosen Produkte gebotene Schutz für die meisten Privatanwender völlig ausreichend sein. Hinzu kommt, dass viele Entwickler kostenloser Antivirenprogramme die Engines der großen Hersteller lizensieren und somit einen durchaus effektiven Schutz bieten können.

Ein effektiver Schutz vor Viren muss also nicht zwangsläufig Geld kosten. Zu beachten ist aber, dass die Zusatzfunktionen der kommerziellen Produkte bei den kostenlosen Anbietern häufig fehlen. Dazu gehört insbesondere die Firewall, die das Netzwerk vor Eindringlingen schützt. Auch ausgereifte Funktionen zum Schutz gegen Phishing oder Spam sind in den kostenlosen Angeboten in der Regel nicht enthalten. Die Verwendung eines kostenlosen Virenschutzes stellt also zumindest höhere Anforderungen an den Selbstschutz des Nutzers. Dabei kann es schon ausreichend sein, potenzielle Virenquellen Adressen wie Tauschbörsen, Erotikseiten oder unbekannte E-Mail-Anhänge zu meiden.

5.3 Avast!

Avast! Free Antivirus ist derzeit der mit großem Abstand erfolgreichste kostenlose Virenschutz. Seine Beleibtheit verdankt der Scanner vor allem der Tatsache, dass die Software nicht mit übermäßiger Werbung zugemüllt wird und dem für ein kostenloses Virenprogramm sehr großen Funktionsumfang. Außerdem wurde die Software speziell für den Einsatz auf durchschnittlichen Heimrechnern optimiert, was die Arbeitsgeschwindigkeit beträchtlich erhöht.

5.3.1 Viele kostenlose Funktionen

Avast! bietet viele Funktionen, die in vergleichbaren kostenlosen Produkten nicht enthalten sind. So ermöglicht die Startzeitüberprüfung beispielsweise einen Virenscan während des Bootvorgangs. Diese Funktion bieten nicht einmal alle kommerziellen Produkte. Außerdem erhält der Nutzer ein großes Maß an Kontrolle und kann das Verhalten der Software in vielen detaillierten Einstellungen an seinen eigenen Geschmack anpassen. Innovativ ist auch der Browserschutz, bei dem neben der Adressleiste des Browsers die Sicherheit der besuchten Webseite bewertet wird, wobei Avast! vor allem auf Beurteilungen der Nutzer setzt.

5.3.2 Zusatzfunktionen kosten extra

Neben dem kostenlosen Antivirenprogramm bietet Avast! noch einige kostenpflichtigen Suiten wie etwa die Avast! Internet Security, die neben dem Virenprogramm noch eine vollwertige Firewall und Smapschutz bietet. Ausserdem wird unter dem Namen Avast! Pro ein voll ausgestattetes Paket vertrieben, in dem auch eine virtuelle Sandbox enthalten ist.

5.4 Avira

Avira Free Antivirus ist ein in Deutschland entwickeltes, kostenloses Antivirenprogramm und vor allem im deutschsprachigen Raum sehr verbreitet. Der Entwickler gehörte in den 80er Jahren zu den deutschen Pionieren im Bereich der Antivirensoftware. Heute vertreibt die Firma neben dem kostenlosen, werbefinanzierten Virenschutz noch eine Reihe von kostenpflichtigen Programmversionen, die jeweils über verschiedene Zusatzfunktionen verfügen.

Besonders erfolgreich wurde Avira im Jahre 2004, als das kostenlose Antivirenprogramm um einen Schutz vor sogenannten Dialern erweitert wurde. Dialer stellten damals ein großes Sicherheitsproblem dar und kosteten die Opfer viel Geld. Der Dialerschutz von Avira war der erste seiner Art und damals selbst in kommerziellen Virusprogrammen nicht integriert. Lange Zeit war Avira unter den kostenlosen Virenscannern das Produkt mit dem professionellsten Funktionsumfang, erst mit Avast! kam später ein ernstzunehmender Konkurrent auf den Markt.

5.5 Panda Cloud Antivirus

Cloud Antivirus Free ist ein Sicherheitsprogramm der spanischen Firma Panda. Grundsätzlich handelt es sich dabei um ein kostenloses Antivirusprogramm, das sich jedoch in seiner Funktionsweise deutlich von der Konkurrenz unterscheidet. Denn Panda Cloud Antivirus Free arbeitet nicht auf dem Rechner des Nutzers, sondern aus der Cloud. Dadurch wird die Systembelastung nicht nur reduziert, sondern geht quasi gegen Null. Auch die Technik zur Erkennung von Viren ist durchaus innovativ.

5.5.1 Sicherheit in der Cloud

Der Aufbau über eine Cloud Verbindung erlaubt es den Nutzern, Informationen über Bedrohungen oder falsche Alarme in Echtzeit an den Hersteller und über diesen an sämtliche anderen Nutzer zu melden. Dies ermöglicht eine besonders hohe Aktualität von Datenbanken und Signaturen. Allerdings ist zu beachten, dass Panda Cloud Security Free zwangsläufig eine ständige Internetverbindung voraussetzt, die Verwendung der Software macht deshalb nur mit einer Flatrate Sinn.

5.5.2 Sauber und aufgeräumt

Auch bei der Benutzeroberfläche setzt sich Panda Cloud Antivirus deutlich von vielen anderen Antivirenprogrammen ab. Die Benutzeroberfläche erscheint in einem schlichten dunkelgrau, sämtliche wichtigen Informationen werden auf einen Blick angezeigt. Dafür muss der Nutzer jedoch auf einige Zusatzfunktionen und detaillierte Einstellungsmöglichkeiten verzichten.

5.6 Malwarebytes

Malwarebytes ist ein Sicherheitsprogramm für Privatanwender, das sich vor allem auf das Auffinden und Entfernen von sogenannter Malware spezialisiert hat. Zwar findet Malwarebytes auch Viren und Trojaner, in dieser Disziplin kann die Software jedoch nicht mit den vollwertigen Virenscannern mithalten. Dagegen ist die Performance im Bereich der Malware zumindest im kostenlosen Marktsegment unerreicht.

5.6.1 Malwarebytes als Ergänzung

Malwarebytes eignet sich in der kostenlosen Variante hervorragend als Ergänzung zu einem reinen Virenscanner. Selbst wenn die Antivirenprogramme heute meist selbst Funktionen zum Schutz vor Malware an Bord haben, können sie oft nicht mit der Gründlichkeit mithalten, mit der Malwarebytes entsprechende Schadprogramme findet und entfernt. Auch in der Geschwindigkeit des Scannens ist Malwarebytes den Virenscannern weit überlegen, ein vollständiger Systemscan dauert normalerweise nur wenige Minuten. Darüber hinaus ist Malwarebytes zu den meisten Antivirenprogrammen kompatibel, kann also neben einem vollwertigen Virenschutz installiert und genutzt werden.

5.6.2 Malwarebytes Pro

Wie fast alle Anbieter kostenloser Virenprogramme vertreibt auch Malwarebytes einen vollwertigen aber kostenpflichtigen Virenscanner neben der kostenlosen Version. Die Unterschiede der einzelnen Versionen liegen vor allem im Echtzeitschutz, der in der kostenlosen Variante fehlt. Dort können Scans nur manuell gestartet werden.

6 So finden Sie den passenden Virenscanner

Die verschiedenen Produkte für den Virenschutz unterscheiden nicht nur in den Bereichen Erkennungsquote, Reparaturleistung und Systembelastung, sondern auch in den Zusatzleistungen wie Phishing-Schutz, Spamfilter oder Heuristik. Welches dieser Programme nun am besten zu Ihnen passt, hängt vor allem davon ab, wie Sie das Internet nutzen. Grundsätzlich können Sie jedoch mit keinem der Antivirenprogramme etwas falsch machen, alle bekannten Produkte bieten einen effektiven Schutz vor Viren und anderen Gefahren.

6.1 Kostenlos oder kommerziell?

Auch die Frage, ob ein kostenloser Virenschutz ausreichend ist, beschäftigt viele Internetnutzer. Grundsätzlich verwenden die kostenlosen Programme die gleiche Engine wie kommerzielle Angebote, stehen den kostenpflichtigen Angeboten beim Virenschutz also durchaus gleichwertig gegenüber. Wer das Internet jedoch hauptsächlich beruflich nutzt, sollte eher ein paar Euro im Jahr in ein professionelles Produkt investieren. Denn gerade für diese Zielgruppe sind Zusatzfunktionen wie der Schutz des Online Bankings besonders wichtig.

6.2 Ansprüche festlegen

Zunächst sollten Sie überlegen, wie Sie das Internet normalerweise nutzen. Beschränkt sich Ihre Zeit im Netz etwa auf die Erledigung von Home Office Aufgaben und surfen Sie nur auf seriösen Seiten, ist die Gefahr einer Infektion mit bösartigen Programmen eher gering. Hier reicht ein kostenloser Virenschutz in der Regel völlig aus. Nutzen Sie dagegen Online Banking, Tauschbörsen und Chatrooms, sollten Sie Ihren Computer auch professionell absichern.

Von den verschiedenen Qualitätsmerkmalen eines Antivirenprogramms ist die Systemauslastung besonders wichtig. Wenn Sie beispielsweise einen Rechner mit alter Hardware nutzen, können Virenscans schon einmal einige Stunden dauern und den Computer in dieser Zeit deutlich ausbremsen. Auch Gamer oder Nutzer von anderen hardwarehungrigen Anwendungen profitieren von einer möglichst schnellen und unauffälligen Antivirensoftware.

6.3 Demoversionen testen

Für die Nutzung der meisten kommerziellen Antivirenprogramme müssen Sie in der Regel ein einjähriges Abonnement abschließen. Damit Sie die Software zunächst einmal ausgiebig testen können, bieten die meisten Hersteller eine Demoversion zum Download an. Diese lässt sich in der Regel über einen Zeitraum von 30 Tagen ohne Einschränkungen testen. Dadurch haben Sie vor allem die Gelegenheit, die Systemauslastung auf Ihrem Rechner zu testen. Denn dieser Faktor kann stark von der Hardware abhängen und von Computer zu Computer unterschiedlich ausfallen.

Ein Antivirenprogramm gräbt sich sehr tief in das System ein. Wenn Sie bereits einen Virenschutz installiert haben und ein anderes Produkt testen wollen, müssen Sie den alten Virenscanner zuvor unbedingt restlos entfernen. Dazu reicht es in der Regel nicht, das Programm einfach zu deinstallieren. Stattdessen müssen auch alle Einträge in der Registry und sonstige Programmreste entfernt werden. Hierzu bieten fast alle Hersteller entsprechende Deinstallationstools an.

6.4 Unabhängige Tests

Auch die Tests der aktuellen Programmversionen, die regelmäßig in Computerfachzeitschriften oder auf den entsprechenden Webseiten erscheinen, können eine gute Entscheidungshilfe sein. Hier sollten Sie allerdings beachten, dass es sich auch wirklich um unabhängige Tests handelt. Liegt der Zeitschrift zum Beispiel eine Gratisversion eines bestimmten Herstellers bei und kommt dieser Hersteller beim Test im selben Heft auf den ersten Platz, muss das nicht unbedingt ein Zufall sein. Garantiert unabhängig sind dagegen beispielsweise die Tests der Stiftung Warentest.

Speziell zum Test von Antivirenprogrammen wurde das Projekt AV-test.org gestartet. Dieses überprüft mehrmals im Jahr die wichtigsten Produkte für Privatanwender und Unternehmen. Dabei vergibt das Labor Punkte in den Kategorien Erkennungsquote, Reparaturleistung und Systembelastung. Die einzelnen Produkte lassen sich dadurch sehr übersichtlich vergleichen. Allerdings fehlen bei den Tests von AV-test.org Angaben zum Funktionsumfang der getesteten Programme.

7 Fazit

Angesichts der durchaus zahlreichen Gefahren im Internet überrascht es immer wieder, wie viele Menschen sich beim Surfen auf ihr Glück verlassen und ein Antivirenprogramm für überflüssig halten. Dabei sind die Entwickler von Viren, Trojanern und anderer Schadsoftware mittlerweile in der Lage, ihre Angriffe so gut zu tarnen, dass sie selbst

erfahrenen Nutzern nicht auffallen. Ein effektiver Virenschutz ist deshalb eine absolute Grundvoraussetzung für das Surfen im Internet. Das gilt umso mehr, wenn Sie im Internet persönliche und wichtige Informationen wie Bankdaten oder Ihre Kreditkartennummer preisgeben.

7.1 Persönliche und finanzielle Risiken

Ein unentdeckter Angriff auf Ihren Computer kann weitreichende Konsequenzen haben. Wenn der Computer beispielsweise lahm gelegt wird und Sie beruflich auf dessen Nutzung angewiesen sind, kann dies zu Gewinnausfällen führen. Private Dokumente wie Fotos, Steuererklärungen und E-Mails können in den falschen Händen zu peinlichen oder sogar gefährlichen Situationen führen. Von der Gefahr des Missbrauchs von Kreditkarten- und Bankdaten ganz zu schweigen. Gemessen an diesen Risiken ist selbst die Jahresgebühr für ein kommerzielles Antivirenprogramm für die meisten Nutzer eine durchaus lohnenswerte Investition.

7.2 Vernunft als Virenscanner

Allerdings kann auch das beste Virenprogramm nicht die menschliche Vernunft ersetzen. Deshalb sollten sich Internetnutzer stets an grundlegende Sicherheitsregeln halten. Beispielsweise sollten Dateien aus unbekannten Quellen niemals geöffnet werden, persönliche Informationen sollten nur über gesicherte und verschlüsselte Verbindungen übertragen werden. Tauschbörsen erfreuen sich zwar vor allem unter jungen Nutzern großer Beliebtheit, eröffnen Kriminellen aber auch die Möglichkeit, ihre Schadprogramme auf den Rechner des Opfers zu schleusen. Solche Gefahren sollten deshalb entweder ganz gemieden oder nur mit einem Virenscanner im Rücken in Kauf genommen werden.

Bildquelle: blackonix / bigstockphoto.com