

Antivirenprogramm

Ein **Antivirenprogramm**, **Virensscanner** oder **Virenschutz**-Programm (Abkürzung: AV) ist eine Software, die Schadprogramme wie z. B. Computerviren, Computerwürmer oder Trojanische Pferde aufspüren, blockieren und gegebenenfalls beseitigen soll.

Inhaltsverzeichnis

Geschichte

Typen von Antivirenprogrammen

Echtzeitscanner

Manueller Scanner

Online-Virensscanner

Sonstige Scanner

Funktionsweise und Erfolgswahrscheinlichkeit

Scanengines

Heuristik

SandBox

Verhaltensanalyse

Nachträgliche Erkennung

Cloud-Technik

Automatische Aktualisierung

Probleme mit Virenscannern

Kritik an Virenscannern

Überprüfen der Konfiguration des Virensanners

Antivirensoftware

Weblinks

Einzelnachweise

Geschichte

Die meisten der Computerviren, die Anfang und Mitte der 1980er Jahre geschrieben wurden, waren auf reine Selbstreproduktion beschränkt und verfügten oft nicht unbedingt über eine spezifische Schadfunktion. Erst als die Technik der Virenprogrammierung breiteren Kreisen bekannt wurde, tauchten zunehmend Schadprogramme auf, die gezielt Daten auf infizierten Rechnern manipulierten oder zerstörten. Damit war die Notwendigkeit gegeben, sich um die Bekämpfung dieser schädlichen Programme durch spezielle Antivirenprogramme Gedanken zu machen.^[1]

Es gibt konkurrierende Ansprüche, wer der Erfinder des ersten Antivirenprogrammes ist. Das erste Programm zur Bekämpfung des Wurms Creeper im ARPA-Net wurde bereits 1971 entwickelt. Die wahrscheinlich erste öffentlich dokumentierte Entfernung eines Computervirus mit einem Tool wurde von Bernd Fix im Jahr 1987 durchgeführt.^{[2][3]} Fred Cohen, der schon 1984 durch seine Arbeiten das Thema „Computerviren“ öffentlich gemacht hatte,^[4] entwickelte ab 1988 Strategien zur Virenbekämpfung,^[5] die von späteren Antivirenprogrammierern aufgegriffen und fortgeführt wurden.

Ebenfalls 1988 entstand im BITNET/EARN-Rechnerverbund eine Mailingliste namens VIRUS-L,^[6] in der vor allem über das Auftauchen neuer Viren sowie die Möglichkeiten zur Virenbekämpfung diskutiert wurde. Einige Teilnehmer dieser Liste wie zum Beispiel John McAfee oder Eugene Kaspersky gründeten in der Folge Unternehmen, die kommerzielle Antivirenprogramme entwickelten und anboten. Vier Jahre zuvor, 1984, war schon Arcen Data (heute Norman ASA) gegründet worden, das sich Ende der 1980er Jahre, mit dem Auftauchen der ersten Computerviren in Norwegen, ebenfalls auf Antivirenprogramme spezialisierte.^[7] Im Jahr 1987 stellte das Unternehmen G DATA Software das weltweit erste kommerzielle Virenschutzprogramm vor, welches speziell für den Atari ST entwickelt worden ist.^[8] Bevor eine Internet-Anbindung üblich wurde, verbreiteten sich Viren typischerweise über Disketten. Antivirenprogramme wurden zwar manchmal verwendet, aber nur unregelmäßig auf einen aktuellen Stand nachgeführt. Während dieser Zeit prüften Antivirenprogramme nur ausführbare Programme sowie die Boot-Sektoren auf Disketten und Festplatten. Mit der Verbreitung des Internets begannen Viren auf diesem Weg, neue Rechner zu infizieren und damit eine allgemeinere Gefahr darzustellen.^[9]

Mit der Zeit wurde es für Antivirenprogramme immer wichtiger, verschiedene Dateitypen (und nicht nur ausführbare Programme) auf verborgene Viren zu untersuchen. Dies hatte unterschiedliche Gründe:

- Die Verwendung von Makros in Textverarbeitungs-Programmen wie Microsoft Word stellten ein zusätzliches Viren-Risiko dar. Virenprogrammierer begannen, Viren als Makros in Dokumente einzubetten. Dies bedeutete, dass Computer allein dadurch infiziert werden konnten, dass ein eingebettetes Makrovirus in einem Dokument ausgeführt wurde.^[10]
- Spätere E-Mail-Programme, insbesondere Microsoft Outlook Express und Outlook, waren verwundbar für Viren, die in E-Mails eingebunden waren. Dadurch konnte ein Rechner infiziert werden, indem eine E-Mail geöffnet und angesehen wurde.

Mit der steigenden Anzahl vorhandener Viren wurde auch die häufige Aktualisierung der Antivirenprogramme notwendig. Aber selbst unter diesen Umständen konnte sich ein neuartiger Virus innerhalb kurzer Zeit stark verbreiten, bevor die Hersteller von Antivirenprogrammen darauf mit einer Aktualisierung reagieren konnten.^[11]

Typen von Antivirenprogrammen

Echtzeitscanner

Der Echtzeitscanner (englisch *on-access scanner*, *real-time protection*, *background guard*), auch Zugriffsscanner oder residenter Scanner genannt, ist im Hintergrund als Systemdienst (Windows) oder Daemon (Unix) aktiv und scannt alle Dateien, Programme, den Arbeitsspeicher und evtl. den HTTP- wie den FTP-Verkehr. Um dies zu erreichen, werden so genannte Filtertreiber vom Antivirenprogramm installiert, die die Schnittstelle zwischen dem Echtzeitscanner und dem Dateisystem bereitstellen. Findet der Echtzeitscanner etwas Verdächtiges, fragt er in der Regel den Benutzer nach dem weiteren Vorgehen. Dies ist das Blockieren des Zugriffs, das Löschen der Datei, das Verschieben in die Quarantäne oder, wenn möglich, ein Reparaturversuch. Generell kann beim Echtzeitschutz zwischen zwei Strategien unterschieden werden:

1. Scannen beim Öffnen von Dateien (Lesevorgang)
2. Scannen beim Erstellen / Ändern von Dateien (Schreibvorgang)

Es kann der Fall eintreten, dass eine virulente Datei gespeichert wurde, bevor eine Virensignatur für sie verfügbar war. Nach einem Signatur-Update ist es aber möglich, sie beim Öffnen zu erkennen. In diesem Fall ist also ein Scannvorgang beim Öffnen der Datei dem Scannvorgang beim Schreiben der Datei überlegen. Um die Belastung durch den Echtzeitscanner zu verringern, werden oft einige Dateiformate, komprimierte Dateien (Archive) oder Ähnliches nur zum Teil oder gar nicht gescannt.

Manueller Scanner

Der manuelle Scanner (englisch *on-demand scanner*), auch als Dateiscanner bezeichnet, muss vom Benutzer manuell oder zeitgesteuert gestartet werden (On-Demand). Findet ein Scanner schädliche Software, erscheint eine Warnmeldung und in der Regel auch eine Abfrage der gewünschten Aktion: Reinigung, Quarantäne oder Löschung der befallenen Datei(en).

Online-Virens Scanner

Als Online-Virens Scanner werden Antivirenprogramme bezeichnet, die ihren Programmcode und die Viren-Muster über ein Netzwerk (online) laden. Sie arbeiten im Gegensatz zu fest installierten Virens Scannern nur im On-Demand-Modus. Das heißt, der persistente Schutz durch einen On-Access-Modus ist nicht gewährleistet. Oft werden Online-Virens Scanner auch als sogenannte *Second-Opinion-Scanner* benutzt, um sich zusätzlich zum installierten Virens Scanner eine „zweite Meinung“ zu eventuellem Befall einzuholen.

Weiterhin gibt es Webseiten, die es ermöglichen, einzelne Dateien mit verschiedenen Virens Scannern zu prüfen. Für diese Art des Scans muss der Benutzer selbst aktiv die Datei hochladen, es ist also eine Spezialform des *On-Demand-Scan*.

Sonstige Scanner

- Neben dem Echtzeit- und dem manuellen Scanner gibt es noch eine Reihe weiterer Scanner.

Die meisten davon arbeiten, indem sie den Netzwerkverkehr analysieren. Dazu scannen sie den Datenstrom und führen bei einer Auffälligkeit eine definierte Operation aus, wie etwa das Sperren des Datenverkehrs.

- Eine andere Lösung ist der Einsatz von Proxysoftware. Manche Proxys erlauben das Anbinden von Antivirensoftware. Wird eine Datei so heruntergeladen, wird diese zunächst am Proxy untersucht und geprüft, ob sie verseucht ist. Je nach Ergebnis wird sie dann an den Client ausgeliefert oder gesperrt. Ein deutlicher Nachteil besteht jedoch in der Tatsache, dass dies bei einer End-zu-End-Verschlüsselung quasi wirkungslos ist. Eine Variante dieser Proxy-Virusfilter sind Mail-Relay-Server mit Antivirus-Software, teilweise als *Online-Virusfilter* bezeichnet (vgl. aber oben). Dabei werden E-Mails zunächst auf den Relay-Server geleitet, dort gescannt und abgewiesen, unter Quarantäne gestellt oder gesäubert und dann auf den Mailserver des Empfängers weitergeleitet.

Funktionsweise und Erfolgswahrscheinlichkeit

Virens Scanner können prinzipiell nur *bekannte* Schadprogramme (Viren, Würmer, Trojaner etc.) bzw. Schadlogiken (englisch *Evil Intelligence*) erkennen und somit nicht vor allen Viren und Würmern schützen. Daher können Virens Scanner generell nur als Ergänzung zu allgemeinen Vorsichtsmaßnahmen betrachtet werden, die Vorsicht und aufmerksames Handeln bei der Internetnutzung nicht entbehrlich macht. So fand die Stiftung Warentest bei einem „internationalen Gemeinschaftstest“^{[12][13]} von 18 Antivirusprogrammen Anfang 2012 mit 1.800 eingesetzten „aktuellen“ Schädlingen Werte von 36 % bis 96 % aufgespürten Signaturen.^[14] Symantec-Vizechef Brian Dye gestand gegenüber dem Wall Street Journal ein, dass Antivirensoftware nur etwa 45 % aller Angriffe erkenne.^[15]

Grundsätzlich kann bei der Erkennung zwischen zwei Techniken unterschieden werden. Auf Grund der Vor- und Nachteile werden bei aktuellen Virens Scannern beide Techniken eingesetzt, um die Schwächen der jeweils anderen auszugleichen.

- **Reaktiv:** Bei dieser Art der Erkennung wird ein Schädling erst erkannt, wenn eine entsprechende Signatur (oder bekannter Hash-Wert in der Cloud) seitens des Herstellers der Antivirensoftware zur Verfügung gestellt wurde. Dies ist die klassische Art der Virenerkennung, welche von praktisch jeder Antivirensoftware verwendet wird.
 - Vorteil: Eine Signatur kann innerhalb kurzer Zeit erstellt werden und bildet daher immer noch das Rückgrat eines jeden Scanners (bei Onlineverbindungen zusätzlich Cloud-basierte Erkennung)
 - Nachteil: Ohne aktualisierte Signaturen werden keine neuen Schadprogramme erkannt.
- **Proaktiv:** Dies bezeichnet die Erkennung von Malware, ohne dass eine entsprechende Signatur zur Verfügung steht. Aufgrund der rapiden Zunahme neuer Schadprogramme werden solche Techniken immer wichtiger. Proaktive Verfahren sind etwa die Heuristik, Verhaltensanalyse oder die SandBox-Techniken.
 - Vorteil: Erkennung noch unbekannter Schadprogramme.
 - Nachteil: Die komplexe Technik bedarf hoher Entwicklungskosten und langer Entwicklungszyklen. Proaktive Techniken haben prinzipbedingt gegenüber reaktiven eine höhere Fehlalarmquote.

Scanengines

Unter einer Scanengine versteht man den Programmteil eines Virens Scanners, der für die Untersuchung eines Computers oder Netzwerkes auf Schadprogramme verantwortlich ist. Eine Scanengine ist somit unmittelbar für die Effizienz von Antivirensoftware verantwortlich. Für gewöhnlich sind Scanengines Softwaremodule, die unabhängig vom Rest eines Virens Scanners aktualisiert und eingesetzt werden können. Es gibt Antivirensoftware, welche neben der eigenen Scanengine auch lizenzierte Scanengines anderer AV-Hersteller einsetzt. Durch den Einsatz mehrerer Scanengines kann zwar die Erkennungsrate theoretisch gesteigert werden, jedoch führt dies immer zu drastischen Performance-Verlusten. Es bleibt daher fragwürdig, ob sich Virens Scanner mit mehreren Scanengines als sinnvoll erweisen. Das hängt vom Sicherheitsanspruch oder dem Anspruch an Systemperformance ab und muss von Fall zu Fall entschieden werden.

Die Leistungsfähigkeit eines signaturbasierten Antivirens Scanners bei der Erkennung von schädlichen Dateien hängt nicht nur von den verwendeten Virensignaturen ab. Oftmals werden die ausführbaren Dateien vor ihrer Verbreitung so gepackt, dass sie sich später selbst entpacken können (Laufzeitkomprimierung). So kann ein eigentlich bekannter Virus der Erkennung durch manche Scanner entgehen, weil sie nicht in der Lage sind, den Inhalt des laufzeitkomprimierten Archives zu untersuchen. Bei diesen Scannern kann nur das Archiv als solches in die Signaturen aufgenommen werden. Wird das Archiv neu gepackt (ohne den Inhalt zu ändern), müsste dieses Archiv ebenfalls in die Signaturen

aufgenommen werden. Ein Scanner mit der Fähigkeit, möglichst viele Formate entpacken zu können, ist hier im Vorteil, weil er den Inhalt der Archive untersucht. Somit sagt auch die Anzahl der verwendeten Signaturen noch nichts über die Erkennungsleistung aus.

Eine Engine beinhaltet mehrere Module, die je nach Hersteller unterschiedlich implementiert und integriert sind und miteinander interagieren:

- Dateiformat-Analyse (wie Programme (PE, ELF), Scripte (VBS, JavaScript), Datendateien (PDF, GIF))
- Pattern-Matcher (Mustererkennung) für die klassischen Signaturen
- Entpack-Routinen für
 - laufzeitkomprimierte Programme und Verschlüsselungsroutinen (so etwa UPX, Aspack, YodaCrypt)
 - Archive (so ZIP, RAR, 7z, UUE/Base64)
 - Mailbox-Formate (so mbox, .dbx, .eml, MIME)
- Code-Emulation (vergleichbar mit einer Art *Mini-Sandbox* oder es greift eine Sandbox darauf zurück, nützlich für generische Erkennung oder bei polymorphen Schadprogrammen)
- Heuristik für unterschiedliche Typen (PE, Scripte, Makros)
- diverse Filter (in ELF-Dateien muss nicht nach PE-Signaturen gesucht werden oder per Zugriffsschutz geblockte Dateien – entweder vordefinierte Regeln oder selbst konfiguriert)

Weiters oder vorrangig beim Echtzeitschutz eingesetzt:

- Verhaltensanalyse
- Cloud-Technik
- Sandbox

Heuristik

Einige Virens Scanner verfügen über die Möglichkeit, auch nach allgemeinen Merkmalen zu suchen (Heuristik),^[13] um unbekannte Viren zu erkennen, oder sie bringen ein rudimentäres Intrusion Detection System (IDS) mit. Die Wichtigkeit dieser – präventiven – Art der Erkennung nimmt stetig zu, da die Zeiträume, in denen neue Viren und Varianten eines Virus in Umlauf gebracht werden (auf den Markt drängen), immer kürzer werden. Für die Antivirenhersteller wird es somit immer aufwändiger und schwieriger, alle Schädlinge zeitnah durch eine entsprechende Signatur zu erkennen. Heuristika sollten nur als Zusatzfunktion des Virens Scanners angesehen werden. Die tatsächliche Erkennung noch unbekannter Schadprogramme ist eher gering, da die Schadprogramm-Autoren meistens ihre „Werke“ mit den bekanntesten Scannern testen und sie so ändern, dass sie nicht mehr erkannt werden.

SandBox

Um die Erkennung von unbekannten Viren und Würmern zu erhöhen, wurde von dem norwegischen Antivirenhersteller Norman im Jahr 2001 eine neue Technik vorgestellt, bei der die Programme in einer gesicherten Umgebung, der Sandbox, ausgeführt werden. Dieses System funktioniert, vereinfacht ausgedrückt, wie ein Computer im Computer. In dieser Umgebung wird die Datei ausgeführt und analysiert, welche Aktionen sie ausführt. Bei Bedarf kann die Sandbox auch Netzwerkfunktionalitäten, etwa eines Mail- oder IRC-Servers, bereitstellen. Die Sandbox erwartet bei der Ausführung der Datei eine

für diese Datei typische Verhaltensweise. Weicht die Datei von dieser zu einem gewissen Grad ab, klassifiziert die Sandbox diese als potentielle Gefahr. Dabei kann sie folgende Gefährdungen unterscheiden:

- W32/Malware
- W32/EMailWorm
- W32/NetworkWorm
- W32/BackDoor
- W32/P2PWorm
- W32/FileInfector
- W32/Dialer
- W32/Downloader
- W32/Spyware

Als Ergebnis liefert sie zudem eine Ausgabe, die zeigt, welche Aktionen die Datei auf dem System ausgeführt hätte und welcher Schaden angerichtet worden wäre. Diese Information kann aber auch nützlich sein, um eine Bereinigung eines infizierten Computersystems vorzunehmen. Durch die Technik der Sandbox konnten nach Tests von AV-Test^[16] 39 % noch unbekannter Viren und Würmer erkannt werden, bevor eine Signatur bereitstand. Im Vergleich zu einer herkömmlichen Heuristik ist dies ein wirklicher Fortschritt in proaktiver Erkennung. Nachteil der Sandbox-Technik ist, dass sie durch die Code-Emulation recht ressourcen-intensiv und langsamer als klassisches Signaturescannen ist. Daher wird sie primär in den Labors der Antiviren-Hersteller verwendet, um die Analyse- und damit die Reaktionszeit zu verbessern.

Ähnlich wie bei Online-Scannern stellen verschiedene Anbieter Web-Oberflächen ihrer Sandboxes zur Analyse einzelner verdächtiger Dateien zur Verfügung (normalerweise Basisfunktionen kostenlos, erweiterte Funktionen gegen Entgelt).^{[17][18][19][20][21][22][23][24]}

Verhaltensanalyse

Die Verhaltensanalyse (englisch Behavior Analysis/Blocking, oft auch als Hostbased Intrusion Detection System bezeichnet, vgl. NIDS) soll ähnlich wie SandBox und Heuristik anhand von typischen Verhaltensweisen Schadprogramme erkennen und blockieren. Allerdings wird die Verhaltensanalyse nur bei der Echtzeitüberwachung eingesetzt, da dabei die Aktionen eines Programms – im Gegensatz zur Sandbox – auf dem echten Computer mitverfolgt werden, und kann vor Überschreiten einer *Reizschwelle* (Summe der verdächtigen Aktionen) oder bei Verstößen gegen bestimmte Regeln, vor offensichtlich destruktiven Aktionen (Festplatte formatieren, Systemdateien löschen) einschreiten. Bei der Verhaltensanalyse wird oft mit Statistik (Bayes Spamfilter), neuronalen Netzwerken, genetischen Algorithmen oder anderen „trainierbaren/lernfähigen“ Algorithmen gearbeitet.

Nachträgliche Erkennung

Einen neuartigen Ansatz verfolgt der Münchner IT-Dienstleister Retarus mit seiner Lösung Patient Zero Detection. Diese bildet Hash-Werte über alle Anhänge von E-Mails, die über die Infrastruktur des IT-Dienstleisters ankommen, und schreibt sie in eine Datenbank. Wird zu einem späteren Zeitpunkt ein identischer Anhang von einem Scanner als virenverseucht aussortiert, können die zuvor bereits mit dem Schadcode zugestellten Nachrichten anhand der Prüfsumme nachträglich identifiziert und dann Administrator und Empfänger umgehend benachrichtigt werden. Wurden die infizierten Mails noch nicht geöffnet, lassen sie sich ungelesen löschen; in jedem Fall wird die IT-Forensik erleichtert^[25].

Cloud-Technik

Der prinzipielle Unterschied der Cloud-Technik (dt. ‚Wolke‘) zu „normalen“ Scannern ist, dass die Signaturen „in der Cloud“ (auf den Servern der Hersteller) liegen und nicht auf der lokalen Festplatte des eigenen Computers oder auch in der Art der Signaturen (Hash-Werte statt klassischer Virensignaturen wie Bytefolge ABCD an Position 123). Die Signaturen werden nicht bei allen Produkten lokal zwischengespeichert,^[26] so dass ohne Internetverbindung nur eine reduzierte oder keine Erkennungsleistung verfügbar ist. Manche Hersteller bieten für Unternehmen eine Art „Cloud Proxy“ an, der Hash-Werte lokal zwischenpuffert. Ein großer Vorteil der Cloud-Technik ist die Reaktion nahezu in Echtzeit. Die Hersteller verfolgen unterschiedliche Ansätze. Bekannt sind die Programme Panda Cloud Antivirus^[27] (arbeitet inzwischen mit einem lokalen Cache^[28]), McAfee Global Threat Intelligence – GTI (früher Artemis),^[29] F-Secure Realtime Protection Network,^[30] Microsoft *Morro* SpyNet^[31] und Immunet ClamAV für Windows^[32] sowie Symantec mit Nortons SONAR 3 und das Kaspersky Security Network.^[33]

1. Die Mehrheit der Hersteller übertragen lediglich Hash-Werte. Das heißt, wenn sich die Datei eines (Schad)programms nur um 1 Bit ändert, wird es nicht mehr erkannt. Bis dato ist nicht bekannt (wobei es aber anzunehmen ist), ob Hersteller ebenfalls „unscharfe“ Hashes (z. B. ssdeep^[34]) einsetzen, die eine gewisse Toleranz erlauben.
2. Es werden Fehlerkennungen minimiert, da die White- und Blacklists bei den Herstellern ständig mit neuen Hash-Werten von Dateien aktualisiert werden.
3. Ressourceneinsparung: Bereits analysierte Dateien werden nicht mehr erneut aufwendig in einen Emulator oder Sandbox beim Endbenutzer am Computer analysiert.
4. Statistische Auswertung der Ergebnisse beim Hersteller: Von Symantec ist bekannt, dass Hash-Werte von neuen, unbekannten und wenig verbreiteten Dateien als verdächtig eingestuft werden. Unrühmliche Bekanntheit hat diese Funktion unter anderem bei Firefox-Aktualisierungen erlangt.^[35]

Automatische Aktualisierung

Die sogenannte Auto-, Internet- oder auch Live-Updatefunktion, mit der automatisch beim Hersteller aktuelle Virensignaturen heruntergeladen werden, ist bei Virenscannern von besonderer Bedeutung. Wenn sie aktiviert ist, wird der Benutzer regelmäßig daran erinnert, nach aktuellen Updates zu suchen, oder die Software sucht selbstständig danach. Es empfiehlt sich, diese Option zu nutzen, um sicherzugehen, dass das Programm wirklich auf dem aktuellen Stand ist.

Probleme mit Virenscannern

Da Virenscanner sehr tief ins System eingreifen, kommt es bei einigen Anwendungen zu Problemen, wenn sie gescannt werden. Zumeist kommen diese Probleme beim Echtzeitscan zum Tragen. Um Komplikationen mit diesen Anwendungen zu verhindern, erlauben die meisten Virenscanner das Führen einer Ausschlussliste, in der definiert werden kann, welche Daten nicht vom Echtzeitscanner überwacht werden sollen. Häufige Probleme treten auf mit:

- Zeitkritischen Anwendungen: Da die Daten immer erst gescannt werden, entsteht eine gewisse Verzögerung. Für einige Applikationen ist diese zu groß und sie erzeugen Fehlermeldungen oder Funktionsstörungen. Besonders häufig tritt dieses Verhalten auf, wenn auf Daten über eine Netzwerkfreigabe zugegriffen wird und an diesem entfernten Rechner ebenfalls eine Antivirensoftware läuft.

- Datenbanken (jeglicher Art): Da auf Datenbanken für gewöhnlich ein ständiger Zugriff stattfindet und sie oftmals sehr groß sind, versucht der Echtzeitscanner, diese dauerhaft zu scannen. Dies kann zu Timeout-Problemen, ansteigender Systemlast, Beschädigungen der Datenbank bis hin zum völligen Stillstand des jeweiligen Computersystems führen.
- Mailserver: Viele Mailserver speichern E-Mails MIME- oder ähnlich codiert auf der Festplatte ab. Viele Echtzeitscanner können diese Dateien decodieren und Viren entfernen. Da der E-Mailserver jedoch von dieser Entfernung nichts wissen kann, „vermisst“ er diese Datei, was ebenfalls zu Funktionsstörungen führen kann.
- Parsing: Weil Antivirensoftware viele verschiedene, teils unbekannte Dateiformate mit Hilfe eines Parsers untersucht, kann sie selbst zum Ziel von Angreifern werden.^{[36][37]}
- Häufig erlauben es Virens Scanner nicht, noch einen zweiten Virens Scanner parallel auszuführen.
- False Positives, also Fehllarme, die bei einigen Virens Scannern zu einer automatischen Löschung, Umbenennung etc. führen und teilweise nur sehr schwer abzustellen sind. Nach einer Rückumbenennung „erkennt“ das Programm erneut diese Datei und benennt sie wieder um.

Kritik an Virens Scannern

Die Zuverlässigkeit und Wirksamkeit von Virens Scannern wird oft angezweifelt. So vertrauen nach einer Umfrage aus dem Jahr 2009 drei Viertel der befragten Systemadministratoren (Admins) oder Netzwerkbetreuer den Virens Scannern nicht. Hauptgrund sei die tägliche Flut neuester unterschiedlichster Varianten von Schädlingen, die das Erstellen und Verteilen von Signaturen immer unpraktikabler machten. 40 Prozent der befragten Administratoren hatten bereits darüber nachgedacht, die Virens Scanner zu entfernen, weil diese die Performance des Systems negativ beeinflussen. Vielfach werden Virens Scanner eingesetzt, weil die Unternehmensrichtlinien dieses forderten, so die Umfrage.^[38] Diese Studie wurde allerdings von einem Unternehmen in Auftrag gegeben, das eine konkurrierende Software vertrieb, die anhand von Positivlisten das Ausführen von Programmen erlaubt. Dieser „Whitelisting“-Ansatz hat je nach Einsatzgebiet ebenso Vor- und Nachteile.^{[39][40]} Im Jahr 2008 sagte Eva Chen, CEO von Trend Micro, dass die Hersteller von Antivirenprogrammen die Wirksamkeit ihrer Produkte seit 20 Jahren übertrieben und ihre Kunden damit angelogen hätten. Sinngemäß: Kein Antivirusprogramm könne alle Viren blockieren, dafür gäbe es zu viele.^[41]

Eine Sicherheitsstudie ergab 2014, dass nahezu alle untersuchten Antivirenprogramme verschiedenste Fehler aufweisen und damit teilweise die Systeme, auf denen sie installiert sind, angreifbar machen.^{[42][43]}

Das BSI fasst die grundlegende Problematik des Einsatzes von Virens Scannern wie folgt zusammen:














„Antivirensoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, verfügt über weitreichende Systemberechtigungen und muss systembedingt (zumindest für Aktualisierungen) eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten. Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz eines Herstellers sowie seiner authentischen Handlungsfähigkeit entscheidend für den sicheren Einsatz solcher Systeme. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur.“^[44]

Überprüfen der Konfiguration des Virens Scanners

Die Funktion des Virenschanners kann nach der Installation und nach größeren Systemupdates überprüft werden. Damit kein „echter“ Virus zum Test der Virenschanner-Konfiguration verwendet werden muss, hat das *European Institute of Computer Anti-virus Research* in Verbindung mit den Virenschanner-Herstellern die sogenannte *EICAR-Testdatei* entwickelt. Sie ist kein Virus, wird aber von jedem namhaften Virenschanner als Virus erkannt. Mit dieser Datei kann getestet werden, ob das Antivirenprogramm korrekt eingerichtet ist und ob alle Arbeitsschritte des Virenschanners tadellos arbeiten.

Antivirensoftware

Antivirensoftware gibt es kostenlos oder als kostenpflichtige Angebote. Häufig bieten kommerzielle Hersteller auch kostenlose Versionen mit abgespecktem Funktionsumfang an.^[45] Die Stiftung Warentest kam im Frühjahr 2017 zum Ergebnis, dass es guten Schutz mittels Sicherheitssoftware auch kostenlos gibt.^[46] Die folgende Tabelle gibt nur einen kleinen Überblick über ein paar relevante Hersteller, Produkte und Marken.

Hersteller	Relevante Produkte / Marken	Angebote für die folgenden Plattformen	Lizenz	deutschsprachig	darunter kostenlose Angebote
 Avira	Avira Antivirus	Windows , macOS , Android , iOS	Proprietär	ja	ja
 Avast	Avast Antivirus	Windows , macOS , Android , iOS	Proprietär	ja	ja
	AVG Antivirus	Windows , macOS , Android	Proprietär	ja	ja
 Bitdefender	Bitdefender Antivirus	Windows , macOS , Android	Proprietär	ja	ja
 Cisco	ClamAV	Windows , Unixähnliche (darunter Linux)	GPL	nein	ja
 Emsisoft	Emsisoft Anti-Malware	Windows , Android	Proprietär	ja	nein
 ESET	ESET NOD32 Antivirus	Windows , macOS , Linux , Android	Proprietär	ja	nein
 F-Secure Corporation	F-Secure Anti-Virus	Windows , macOS , Android	Proprietär	ja	nein
 G Data CyberDefense	G Data Antivirus	Windows , macOS , Android , iOS	Proprietär	ja	nein
 Kaspersky Lab	Kaspersky Anti-Virus	Windows , macOS , Android , iOS	Proprietär	ja	ja
 Malwarebytes Inc.	Malwarebytes	Windows , macOS , Android	Proprietär	ja	ja
 McAfee	McAfee VirusScan	Windows , macOS , Android , iOS	Proprietär	ja	nein
 Microsoft	Microsoft Defender	Windows	Proprietär	ja	ja
 NortonLifeLock (ehemals Symantec)	Norton AntiVirus	Windows , macOS , Android , iOS	Proprietär	ja	nein

Weblinks

- Robert A. Gehring: Ein Immunsystem für den Computer (<https://web.archive.org/web/20090905003937/http://www.verbraucher-sicher-online.de/artikel/ein-immunsystem-fuer-den-computer>) (Memento vom 5. September 2009 im *Internet Archive*), in: Verbraucher sicher online. (durch das BMELV gefördertes Projekt der Technischen Universität Berlin)

Einzelnachweise

1. Eine kurze Geschichte der Viren (<https://web.archive.org/web/20110212084313/http://www.computerviren-info.de:80/Geschichte.html>) (Memento vom 12. Februar 2011 im *Internet Archive*) auf computerviren-info.de
2. Kaspersky Lab Virus list (<https://web.archive.org/web/20090713091733/http://www.viruslist.com/en/viruses/encyclopedia?chapter=153311150>) (Memento vom 13. Juli 2009 im *Internet Archive*) (englisch)
3. Joe Wells: *Virus timeline* (<https://web.archive.org/web/20121022210552/http://www.research.ibm.com/antivirus/timeline.htm>) (englisch) IBM. 30. August 1996. Archiviert vom Original (<https://giftbot.toolforge.org/deref.fcgi?url=http%3A%2F%2Fwww.research.ibm.com%2Fantivirus%2Ftimeline.htm>) am 22. Oktober 2012. Abgerufen am 6. Juni 2008.
4. [eecs.umich.edu](https://web.eecs.umich.edu/~aparaksh/eecs588/handouts/cohen-viruses.html) (<https://web.eecs.umich.edu/~aparaksh/eecs588/handouts/cohen-viruses.html>) Fred Cohen 1984 „Computer Viruses – Theory and Experiments“ (englisch)
5. Fred Cohen: On the implications of Computer Viruses and Methods of Defense (<https://dl.acm.org/doi/10.1016/0167-4048%2888%2990334-3>) portal.acm.org, 1988 (englisch)
6. Archiv der Mailingliste VIRUS-L. (https://web.archive.org/web/20200910134240/http://securitydigest.org/virus/mirror/www.phreak.org-virus_l/) (Memento vom 10. September 2020 im *Internet Archive*), securitydigest.org (englisch)
7. download.norman.no (http://download.norman.no/documents/timeline_2009.pdf) (PDF; 901 kB) Zeitleiste auf der Seite von Norman ASA (englisch)
8. Hubert Popiolek, Dany Dewitz: *Virenschutz made in Germany: Das steht hinter G Data*. (<https://web.archive.org/web/20210519171635/https://www.computerbild.de/artikel/cb-Special-G-Data-Internet-Security-CBE-10011799.html>) Computer Bild, 22. Mai 2015, archiviert vom Original (<https://giftbot.toolforge.org/deref.fcgi?url=http%3A%2F%2Fwww.computerbild.de%2Fartikel%2Fcb-Special-G-Data-Internet-Security-CBE-10011799.html>) am 19. Mai 2021; abgerufen am 19. Mai 2021.
9. *(I) Evolution of computer viruses* (<https://web.archive.org/web/20090802042225/http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=4974&entorno=&ver=&pagina=&producto=>). Panda Security. April 2004. Archiviert vom Original (<https://giftbot.toolforge.org/deref.fcgi?url=http%3A%2F%2Fwww.pandasecurity.com%2Fhomeusers%2Fmedia%2Fpress-releases%2Fviewnews%3Fnoticia%3D4974%26entorno%3D%26ver%3D%26pagina%3D%26producto%3D>) am 2. August 2009. Abgerufen am 20. Juni 2009.
10. Peter Szor: *The Art of Computer Virus Research and Defense*. Addison-Wesley, 2005, ISBN 0-321-30454-3, S. 66–67.
11. *Protecting Microsoft Outlook against Viruses* (<https://www.slipstick.com/outlook/protecting-outlook-against-viruses/>). Slipstick Systems. February 2009. Abgerufen am 18. Juni 2009.
12. *Antivirushersteller über Stiftung Warentest verstimmt*. (<https://www.heise.de/security/meldung/Antivirushersteller-ueber-Stiftung-Warentest-verstimmt-1500396.html>) 4. April 2012, abgerufen am 11. September 2012.
13. *Das Antivirus-Lexikon: Was bedeutet eigentlich...* (<https://www.heise.de/security/artikel/Das-Antivirus-Lexikon-Was-bedeutet-eigentlich-1105792.html>) In: *heise Security*. Abgerufen am 6. März 2018.

14. *Angriff aus dem Internet*. (<https://web.archive.org/web/20170823162855/https://www.test.de/Antivirenprogramme-Angriff-aus-dem-Internet-4348485-0/>) 13. April 2012, archiviert vom Original (<https://giftbot.toolforge.org/deref.fcgi?url=http%3A%2F%2Fwww.test.de%2FAntivirenprogramme-Angriff-aus-dem-Internet-4348485-0%2F>) am 23. August 2017; abgerufen am 11. September 2012.
15. Jörg Thoma: *Symantec-Vizechef Brian Dye – Antivirensoftware erkennt nur etwa 45 % aller Angriffe*. (<https://www.golem.de/news/symantec-antivirensoftware-ist-tot-1405-106251.html>) golem.de; abgerufen am 5. Mai 2014
16. Testbericht von 2004 auf av-test.org, ZIP-Format (https://web.archive.org/web/20060206144903/http://www.av-test.org/down/papers/2004-09_vb_2004.zip) (Memento vom 6. Februar 2006 im *Internet Archive*)
17. ISecLab (<https://iseclab.org/>)
18. Anubis (<https://web.archive.org/web/20120621053339/http://anubis.iseclab.org/>) (Memento vom 21. Juni 2012 im *Internet Archive*)
19. Wepawet (<https://web.archive.org/web/20090317041224/http://wepawet.iseclab.org/>) (Memento vom 17. März 2009 im *Internet Archive*) (Projekt der TU-Wien, Eurecom France und UC Santa Barbara)
20. ZeroWINE (<http://zerowine.sourceforge.net/>) (Open-Source)
21. Norman Sandbox (https://web.archive.org/web/20091019112118/http://www.norman.com/security_center/security_tools/submit_file) (Memento vom 19. Oktober 2009 im *Internet Archive*)
22. CWSandbox (<https://cwsandbox.org/>)
23. ThreatExpert (<https://threatexpert.de.uptodown.com/windows>)
24. Joebox (<https://web.archive.org/web/20101217080907/http://www.joebox.ch/submit.php>) (Memento vom 17. Dezember 2010 im *Internet Archive*)
25. Malte Jeschke: *E-Mail-Sicherheit: Den Patient Zero identifizieren* (<https://www.computerweekly.com/de/news/450412138/E-Mail-Sicherheit-Den-Patient-Zero-identifizieren>). TechTarget. 1. Februar 2017. Abgerufen am 8. März 2017.
26. Jürgen Schmidt: *Schutzbehauptung*. In: *c't Magazin*. Nr. 2, 2009, S. 77 (Auszug auf [heise.de](https://www.heise.de/ct/artikel/Schutzbehauptung-291854.html) (<https://www.heise.de/ct/artikel/Schutzbehauptung-291854.html>)).
27. Website von Panda Security (<https://www.pandasecurity.com/de/homeusers/vpn/>)
28. Pedro Bustamante: *Arguments against cloud-based antivirus – A cloud-based antivirus needs to check everything against the cloud. Takes more time* (<https://www.pandasecurity.com/en/mediacenter/malware/arguments-against-cloud-based-antivirus/>). Panda. 1. Dezember 2009. Abgerufen am 21. Juni 2010.
29. McAfee Global Threat Intelligence Technology (<https://web.archive.org/web/20101223122411/http://www.mcafee.com/us/mcafee-labs/technology/global-threat-intelligence-technology.aspx>) (Memento vom 23. Dezember 2010 im *Internet Archive*)
30. DeepGuard – Der schnellste Schutz in der Online-Welt (https://web.archive.org/web/20100406020326/http://www.f-secure.com/de_DE/products/technologies/deepguard/) (Memento vom 6. April 2010 im *Internet Archive*)
31. *Microsoft veröffentlicht Beta-Version seiner kostenlosen Antivirenlösung* (<https://www.heise.de/security/meldung/Microsoft-veroeffentlicht-Beta-Version-seiner-kostenlosen-Antivirenloesung-185819.html>). In: *heise.de* vom 24. Juni 2009
32. Clam AV: Windows Antivirus (<https://web.archive.org/web/20111213102530/http://www.clamav.net/lang/de/about/win32/>) (Memento vom 13. Dezember 2011 im *Internet Archive*)
33. [media.kasperskycontenthub.com](https://media.kasperskycontenthub.com/wp-content/uploads/sites/62/2017/10/21140410/Kaspersky_Lab_Whitepaper_KSN_DE_1709.pdf) (https://media.kasperskycontenthub.com/wp-content/uploads/sites/62/2017/10/21140410/Kaspersky_Lab_Whitepaper_KSN_DE_1709.pdf)
34. ssdeep (<https://ssdeep-project.github.io/ssdeep/>)

35. *Norton-Fehlalarm bei Firefox-Update* (<https://www.heise.de/newsticker/meldung/Norton-Fehlalarm-bei-Firefox-Update-1029971.html>). Heise. 28. Juni 2010. Abgerufen am 27. Februar 2011.
36. Katharina Friedmann: *Virens Scanner öffnen Hackern die Türen*. (<https://www.computerwoche.de/a/virens-scanner-oeffnen-hackern-die-tueren,1848636>) Computerwoche, 26. November 2007, abgerufen am 25. Dezember 2021.
37. *Anti-Virus Parsing Engines*. In: nruns.com, 2007 (<https://web.archive.org/web/20080709040624/http://www.nruns.com/parsing-engines-advisories.php>) (Memento vom 9. Juli 2008 im Internet Archive)
38. *Drei Viertel der Admins trauen dem Virens Scanner nicht*. (<https://www.heise.de/newsticker/meldung/Drei-Viertel-der-Admins-trauen-dem-Virens-Scanner-nicht-755737.html>) In: heise.de vom 14. September 2009
39. *anti-virus-rants - the rise of whitelisting*. (<http://anti-virus-rants.blogspot.com/2006/03/rise-of-whitelisting.html>) In: anti-virus-rants.blogspot.com vom 29. März 2006
40. *welivesecurity.com* (<https://www.welivesecurity.com/2008/11/16/white-listing-the-end-of-antivirus/>)
41. Tom Espiner: *Trend Micro: Antivirus industry lied for 20 years* (<https://www.zdnet.com/article/trend-micro-antivirus-industry-lied-for-20-years/>). ZDNet. 30. Juni 2008. Abgerufen am 25. Dezember 2018.
42. Kim Rixecker: *Sicherheitsstudie: Virens Scanner machen Rechner angreifbar*. (<https://web.archive.org/web/20140802030839/http://t3n.de/news/sicherheitsstudie-virens-scanner-antivirens-oftware-560067/>) t3n.de, 30. Juli 2014.
43. Joxean Koret: *Breaking Antivirus Software*. (https://ia801306.us.archive.org/26/items/SyScanArchiveInfocon/SyScan%202014%20Singapore/SyScan%202014%20presentations/SyScan2014_JoxeanKoret_BreakingAntivirusSoftware.pdf) (PDF; 1,3 MB) COSEINC, SYSCAN 360, 2014.
44. publisher: *BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten*. (https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html?nn=520690) Abgerufen am 15. März 2022.
45. *Welches Virenschutzprogramm ist empfehlenswert?* (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Virenschutzprogramme/virenschutzprogramme_node.html#doc504492bodyText3) Bundesamt für Sicherheit in der Informationstechnik, abgerufen am 7. Juni 2021.
46. *Sicherheitssoftware Auch Gratisprogramme bieten guten Schutz*. (<https://www.test.de/presse/pressemitteilungen/Sicherheitssoftware-Auch-GGratisprogramme-bieten-guten-Schutz-5144999-0/>) Stiftung Warentest, 22. Februar 2017, abgerufen am 25. Dezember 2021.

Abgerufen von „<https://de.wikipedia.org/w/index.php?title=Antivirenprogramm&oldid=221191685>“

Diese Seite wurde zuletzt am 16. März 2022 um 17:08 Uhr bearbeitet.

Der Text ist unter der Lizenz „Creative Commons Attribution/Share Alike“ verfügbar; Informationen zu den Urhebern und zum Lizenzstatus eingebundener Mediendateien (etwa Bilder oder Videos) können im Regelfall durch Anklicken dieser abgerufen werden. Möglicherweise unterliegen die Inhalte jeweils zusätzlichen Bedingungen. Durch die Nutzung dieser Website erklären Sie sich mit den Nutzungsbedingungen und der Datenschutzrichtlinie einverstanden.

Wikipedia® ist eine eingetragene Marke der Wikimedia Foundation Inc.