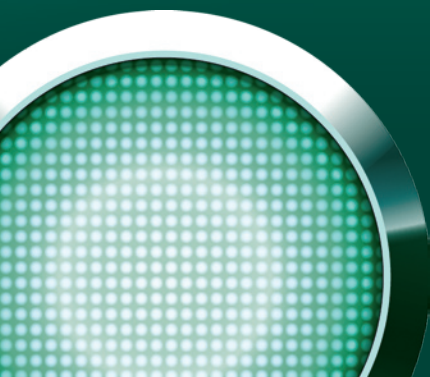


**KASPERSKY** 

W H I T E P A P E R

**Antiviren-Technologien  
im Überblick**



Dieses Whitepaper beleuchtet, mit welchen Methoden sich schädlicher Programmcode identifizieren lässt und zeigt, welche funktionellen und chronologischen Verbindungen zwischen den Schadprogrammen bestehen. Auch ihre technologischen und anwendungsorientierten Besonderheiten werden berücksichtigt. Zwar verwenden nicht nur Antiviren-Programme, sondern auch zahlreiche IT-Sicherheitssysteme die hier beschriebenen Technologien und Prinzipien. Da einige ihrer Funktionen wie das Entpacken komprimierter Programme oder die fließende Signaturerkennung aber Spezialfälle darstellen, bleiben sie im Folgenden unbeachtet.

Zum Aufspüren schädlicher Programme analysierte man früher nur ihre Signaturen. Das sind Bestandteile des Codes, über die sich Malware identifizieren lässt. In dem Maße, in dem sich die Viren weiterentwickelten, verbesserten sich auch die Antiviren-Technologien. Inzwischen setzen die Hersteller von Antiviren-Software vermehrt auf nicht signaturbasierte Verfahren, darunter unterschiedliche Arten der Heuristik.

Anders als die Überschrift vermuten lässt, behandelt dieses Whitepaper nicht sämtliche Antiviren-Strategien im Detail. Vor allem signaturbasierte Verfahren sind so primitiv und eindeutig, dass es praktisch nichts mehr über sie zu sagen gibt. Ganz anders sieht es bei nicht signaturbasierten Technologien aus. Viele Anwender wissen nicht, was sich hinter Bezeichnungen wie „Heuristik“, „proaktive Entdeckung“, „verhaltensorientierte Entdeckung“ oder „HIPS“ verbirgt. Ebenso ist es oftmals unklar, wie sich die Technologien zueinander verhalten, und welche Vor- und Nachteile sie haben.

Dieses Whitepaper will das dazu notwendige Hintergrundwissen vermitteln und richtet sich an diejenigen Leser, die nur eine allgemeine Vorstellung von Antiviren-Technologien haben. Im Folgenden wird gezeigt, wie Schadprogramme funktionieren, und welche Strategien sie gegen Malware einsetzen.

## Aufbau eines Malware-Schutzsystems

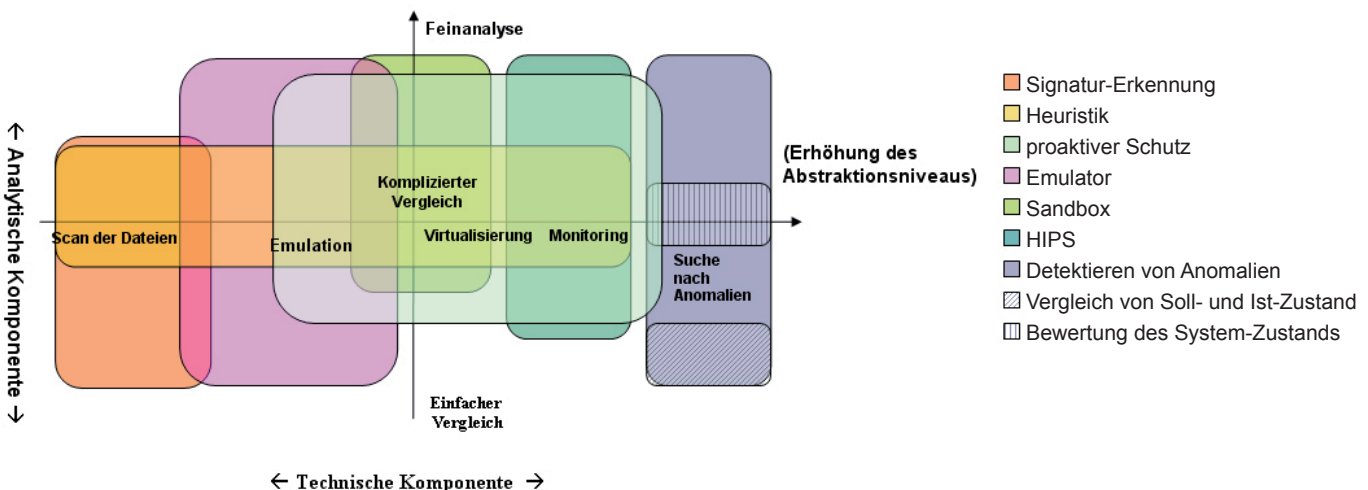
Jeder beliebige Schutzmechanismus lässt sich auf eine technische und eine analytische Komponente reduzieren. Beide können die gleichen Module oder Algorithmen verwenden, müssen aber voneinander getrennte Aufgaben erfüllen.

Die technische Komponente umfasst Programmfunktionen und Algorithmen, welche die analytische Komponente mit Daten versorgen. Das kann der Byte-Code einer Datei sein, eine Programm-Aktion, aber auch einzelne Textzeilen oder einfach alles zusammen.

Die analytische Komponente untersucht die ihr gelieferten Daten und klassifiziert sie. Anhand dieser Einteilung startet das Antivirus-Programm oder eine andere Schutzsoftware eine darauf abgestimmte Aktion. Beispielsweise kann das System den Anwender über den Vorfall benachrichtigen und weitere Anweisungen von ihm erwarten. Andere Aktionen laufen dagegen automatisch ab: Das Antivirus-Tool steckt eine verdächtige Datei in Quarantäne oder blockiert nicht genehmigte Handlungen eines Programms.

Ein solches System kommt dann zum Einsatz, wenn ein Antiviren-Programm schädliche Software per Signatur aufspürt. Die technische Komponente überprüft hier das Dateisystem und einzelne Files sowie deren Inhalt. Der analytische Part vergleicht anschließend bestimmte Byte-Folgen mit Viren-Signaturen und schlägt bei einem Treffer Alarm.

Bei dieser Variante kann man das Verhältnis zwischen technischem und analytischem Teil ebenso leicht erkennen wie deren Vor- und Nachteile. Mit Hilfe dieses Modells lassen sich auch die oftmals unklaren Definitionen der verschiedenen Erkennungsmethoden unterscheiden. Zum Beispiel ist die Heuristik zwar eine Methode der Entscheidungsfindung, aber nur eine Spielart der analytischen Komponente und damit keine



eigenständige Technologie. Ebenso handelt es sich bei HIPS (Host Intrusion Prevention System) nur um eine Variante der technischen Komponente, nämlich um eine Datensammel-Methode.

Daraus folgt zum einen, dass sich die Definitionen von technischer und analytischer Komponente formell zwar nicht widersprechen. Zum anderen charakterisieren sie das Verfahren, in dem sie aufeinander treffen, aber nicht eindeutig: Spricht man von Heuristik, bleibt unklar, welche Daten analysiert werden. Und der Begriff HIPS sagt nichts darüber aus, nach welchem Prinzip das System auf Angriffe reagiert.

Der Artikel beschäftigt sich später im Detail mit der heuristischen Methode und dem HIPS-System. Zunächst werden aber die technische und die analytische Verfahrensweise genauer vorgestellt. Im Folgenden geht es um die Methoden der Informationssammlung und -bearbeitung.

### Die technische Komponente

Um Malware aufzuspüren, sammelt ein Antivirus-Programm ständig Daten, die im System kursieren. Solche Informationen entpuppen sich entweder durch ihren Inhalt oder durch bestimmte Aktionen als Schad-Software.

Cyberschädlinge lassen sich mit folgenden Methoden entdecken:

- ① Überwachung eines Programms
- ② Emulation des Programmcodes
- ③ Virtualisierung in der Sandbox
- ④ Überwachen von Systemereignissen
- ⑤ Suche nach System-Anomalien

Obige Gliederung oben entspricht der Vorgehensweise eines Antiviren-Tools. Zunächst beschränkt es sich darauf, Programm-Dateien zu überwachen. Anschließend erforscht es zusätzlich auch die Ereignisse, welche diese auslösen. Und schließlich wird das komplette Betriebssystem auf mögliche Schwachstellen untersucht. Nach genau diesem Schema haben sich auch die Antiviren-Technologien chronologisch entwickelt.

Die vorgestellten Methoden sind allerdings keine etablierten Verfahren, sondern entwickeln sich ständig weiter. Dabei kommt es vor, dass sie ähnliche Schemata verwenden. Beispielsweise kann die Emulation (②) so verlaufen wie die Überwachung eines Programms (①), oder aber der Virtualisierung von Systemfunktionen ähneln (③). Im Folgenden werden alle fünf Methoden genauer betrachtet.

① **Überwachung eines Programms:** Die ersten Antiviren-Tools beschränkten sich darauf, Byte-Folgen einer Datei zu überprüfen. Als Analyse kann man das allerdings kaum bezeichnen. Die Byte-Folgen wurden lediglich mit einer bekannten Signatur verglichen. Die technische Seite dieses Verfahrens ist deshalb interessanter: Beim Suchen nach Schadprogrammen entnimmt das Antiviren-Tool die Analyse-Daten direkt aus den Dateien übergibt sie der technischen Komponente. Dabei arbeitet der Malware-Scanner nur mit dem ursprünglichen Byte-Code der Datei, beobachtet aber nicht deren Verhalten. Diese Methode mutet zwar archaisch an, ist aber keineswegs veraltet und wird von allen modernen Antiviren-Programmen eingesetzt – allerdings schon lange nicht mehr exklusiv, sondern nur als eine von vielen.

② **Emulation des Programmcodes:** Die Emulation behandelt ein Programm nicht mehr nur als simple Ansammlung von Bits und Bytes, sondern berücksichtigt auch von ihm ausgelöste Ereignisse.

Ein Emulator zerlegt den Byte-Code des Programms in einzelne Kommandos und führt sie in einer virtuellen Instanz des Rechners aus. Potenzielle Malware kann in dieser Umgebung keinen Schaden anrichten und gefährdet daher weder Betriebssystem noch Anwenderdaten.

Viele, wahrscheinlich sogar alle Antiviren-Programme setzen auf Emulatoren. Sie ergänzen hauptsächlich einfache Scan-Techniken wie den Signaturvergleich, helfen aber auch bei ausgefeilteren Methoden wie der Sandbox oder der System-Überwachung.

③ **Virtualisierung in der Sandbox:** Die Sandbox setzt auf eine weiterentwickelte Version der Emulation und verwendet dazu Virtualisierungs-Techniken. Und mit „Sandkasten“ ist dieses Verfahren auch treffend bezeichnet: Die Software wird vom restlichen Betriebssystem abgeschirmt und darf nur innerhalb eines genau abgegrenzten Areals agieren. Im Sandkasten kann sie folglich keinen Schaden anrichten. Dadurch kann das Antiviren-Tool das Verhalten des Programms genau analysieren.

Die Grenze zwischen Emulation und Virtualisierung ist fließend. Die erste Technologie bildet ein System nach, um ein Programm darin auszuführen. Im zweiten Fall läuft die Software in einem abgegrenzten Teil des Betriebssystems. Eine virtuelle Umgebung kontrolliert den Datenaustausch zwischen Betriebssystem und Programm. Damit geschieht die Analyse zwar schon nicht mehr auf Dateiebene, berücksichtigt aber immer noch nicht das komplette System.

Antiviren-Programme nutzen weder Emulator noch Sandbox besonders häufig, weil beide Verfahren viele Systemressourcen beanspruchen. Eine Sandbox kann man leicht daran erkennen, dass Aktionen erst mit spürbarer Zeitverzögerung starten. Ein Antiviren-Programm wird daher zeitversetzt reagieren, wenn es in der Sandbox einen Schädling aufgespürt hat.

Virtualisierungs-Techniken werden ständig weiterentwickelt und zunehmend populärer. Antiviren-Tools setzen künftig sicher verstärkt auf Virtualisierungs-Techniken.

- ④ **Überwachen von Systemereignissen:** Die Überwachung von Systemereignissen ist eine „abstraktere“ Analyse-Form. Während Emulator und Sandbox jedes Programm einzeln unter die Lupe nehmen, wird hier das komplette Betriebssystem beobachtet und jedes Ereignis protokolliert. Die Systemüberwachung gibt diese Informationen dann gebündelt an die analytische Komponente weiter.

Die Entwicklung dieses Verfahrens wird derzeit stark vorangetrieben. Einige Antiviren-Programme setzen es ebenso ein wie Tools, die sich auf Systemmonitoring spezialisiert haben. Die Systemüberwachung gehört jedoch nicht zu den sichersten Verfahren, da potentielle Schadprogramme dabei nicht in einem abgegrenzten Bereich, sondern unmittelbar im Betriebssystem ausgeführt werden.

- ⑤ **Suche nach System-Anomalien:** Diese Methode überprüft, ob ein System von einem Schadprogramm infiziert wurde. Sie basiert auf folgenden Grundsätzen:
  - Die Benutzeroberfläche mit all ihren ausführenden Programmen ist ein geschlossenes System.
  - Der Systemstatus kann sich ändern.
  - Wird auf dem System schädlicher Code ausgeführt, ändert sich dessen Zustand auf „ungesund“ und unterscheidet sich von dem Zustand eines „gesunden“, also nicht infizierten Systems.

Ausgehend von diesen Grundsätzen lässt sich der Zustand eines Betriebssystems beurteilen. Um Anomalien aufzudecken, braucht es allerdings ein recht kompliziertes Verfahren. Dabei muss unter anderem festgelegt werden, wie man einen gesunden Systemzustand definiert, wodurch er sich vom infizierten Zustand unterscheidet, und welche Parameter es zu analysieren gilt. Wegen ihrer Komplexität wird diese Methode bislang kaum eingesetzt. Immerhin kann man erste Ansätze davon in einigen Anti-Rootkit-Werkzeugen entdecken, die einen bestimmten Systemzustand zum Vergleich heranziehen.

## Analytische Komponente

Die analytische Komponente eines Antiviren-Programms lässt sich in drei Hauptkategorien aufteilen. Natürlich gibt es auch zahlreiche andere Varianten.

- ▶ **Einfacher Vergleich:** Bei dieser Methode entscheidet ein simpler Vergleich mit einem bestimmten Muster, ob ein Programm als schädlich oder harmlos klassifiziert wird. Malware lässt sich damit anhand einer definierten Byte-Folge erkennen. Eine verdächtige Aktion reicht aber ebenfalls aus, um das Antiviren-Programm zu alarmieren. Das passiert zum Beispiel, wenn ein Programm versucht, kritische Registry-Werte zu ändern oder Einträge im Autostart-Ordner zu modifizieren.
- ▶ **Komplizierter Vergleich:** Hier fällt die Entscheidung erst, nachdem mehrere ähnliche Ereignisse mit den entsprechenden Mustern verglichen wurden. Beispiel: Das Antiviren-Programm erkennt Malware anhand von mehreren Byte-Signaturen, die für sich genommen jeweils unverdächtig sind. Mit dieser Vergleichsmethode lässt sich schädlicher Code auch an den von ihm aufgerufenen API-Funktionen identifizieren.
- ▶ **Expertensystem:** Das Antiviren-Programm identifiziert Malware über eine Datenanalyse, deren Code sich künstlicher Intelligenz bedient. Schädlicher Code wird daher nicht mit fest vorgegebenen Mustern verglichen, sondern mit vielen unterschiedlichen Systemparametern. Am Ende der Analyse bewertet das Expertensystem den Gefährdungsgrad.

## Produktbezeichnungen im Detail erklärt

Dieser Abschnitt zeigt, welche Algorithmen Antiviren-Programme einsetzen, um Schadsoftware aufzuspüren. Zunächst muss man jedoch verstehen, was hinter den Bezeichnungen steckt, mit denen Hersteller ihre Schutzmechanismen anpreisen. Bei Kaspersky Anti-Virus ist das ein „Proaktiver Schutz“, Panda nennt ihn „TruPrevent“, und F-Secure setzt auf „DeepGuard“. Hier beginnt auch das Verwirrspiel: Die Bezeichnungen sagen oftmals gar nichts über die zugrunde liegende Technologie aus und lassen damit viel Raum für Interpretationen. Da passt es ins Bild, dass Hersteller die jeweilige Antiviren-Lösung auf ihren Webseiten zwar wortreich anpreisen, aber kaum etwas über die Technologie verraten.

Einige Hersteller werben mit dem HIPS-System für ihre Produkte und sprechen von proaktiver oder nicht signaturbasierter Technologie. Mit HIPS, einem Host Intrusion Prevention System, hat das in der Regel aber nichts zu tun. Tatsächlich kann sich hinter den Bezeichnungen alles Mögliche verbergen. Wirbt ein Hersteller mit einem heuristischen Schutz, muss das also nicht zwangsläufig zutreffen.

Den meisten Herstellern von Antiviren-Software liegt es sicher fern, ihre Kundschaft zu täuschen. Viel wahrscheinlicher ist, dass es der Verfasser des Werbetextes nicht allzu genau mit den Bezeichnungen genommen hat. Daher sollte man solche Beschreibungen nur mit Vorsicht genießen.

Im Folgenden werden die am weitesten verbreiteten Antiviren-Begriffe genauer erläutert.

- ▶ **Signaturerkennung:** Ein Begriff, den man eigentlich nicht falsch interpretieren kann. Aus technischer Sicht versteht man darunter die Arbeit mit einzelnen Byte-Folgen einer Datei; aus analytischer Sicht handelt es sich um einen einfachen Vergleich. Die Signaturerkennung ist die älteste und zugleich die zuverlässigste Technologie und wird in fast allen Antiviren-Programmen verwendet.
- ▶ **Emulator und Sandbox:** Auch diese beiden Begriffe sind recht unmissverständlich, weil sie beide nur technische Komponenten beschreiben.
- ▶ **Heuristik:** Hier ist es schon nicht mehr so einfach, eine klare Definition zu finden. Prinzipiell handelt es sich bei der Heuristik um die analytische Komponente eines Antiviren-Programms, aber nicht um eine bestimmte Technologie. Bei frühen Antiviren-Lösungen bezeichnete dieser Begriff ein System, das Schädlinge über flexibel vorgegebene Byte-Schablonen erkennt. Wenn man heute von heuristischen Methoden spricht, meint man einen Schutzmechanismus, dessen analytische Komponente eine Datenanalyse einsetzt.
- ▶ **Verhaltensbasierte und proaktive Erkennung:** Beide Begriffe sind alles andere als eindeutig und lassen viel Raum für Spekulationen. Von der heuristischen Methode bis hin zur Systemüberwachung ist hier alles möglich.
- ▶ **HIPS:** Diese Technologie ist zwar genau definiert, wird in vielen Antiviren-Tools aber missverständlich beschrieben. HIPS steht für Host Intrusion Prevention System und kombiniert Systemüberwachung mit einer beliebigen analytischen Komponente. Ein mit HIPS beworbenes Antiviren-Programm kann daher alle möglichen Schutzmechanismen umfassen.

### Vor- und Nachteile der Schutzmechanismen

Die technische Komponente einer Antivirus-Lösung beeinflusst hauptsächlich die Systemauslastung und ist für Sicherheit und Schutz zuständig. Generell gilt hier: Je weniger abstrakt ein Schutzmechanismus, desto risikoloser ist er auch. Allerdings kann man ihn damit auch einfacher umgehen.

- ▶ **Systemauslastung:** Ein Antiviren-Programm beansprucht nicht nur Prozessorzeit, sondern lastet auch den Arbeitsspeicher zu einem bestimmten Grad aus. Besonders Emulation und Virtualisierung fordern viele Systemressourcen und werden nur langsam

ausgeführt. Auch die Systemüberwachung beansprucht den kompletten Rechner.

- ▶ **Sicherheit:** Darunter versteht man, welchen Gefahren Betriebssystem und Anwenderdaten beim Identifizieren potenziell schädlichen Codes ausgesetzt sind. Malware, die nicht in einer virtuellen Umgebung ausgeführt oder emuliert wird, erhöht das Infektionsrisiko.
- ▶ **Schutz:** Je besser ein Antiviren-Produkt direkte Attacken erkennen und abwehren kann, desto sicherer ist das System. Schadprogramme versuchen aber, sich mit verschiedenen Methoden zu tarnen. Malware kommt daher häufig in komprimierter oder polymorpher Form und bedient sich Rootkit-Technologien. Auch gegen Emulation helfen manche Tricks, die in den Code des Schadprogramms eingebaut werden. An einem Systemüberwachungs-Tool kann sich allerdings fast keine Malware vorbeimogeln, da es hier praktisch unmöglich ist, das Verhalten zu verbergen.

Der analytische Aspekt eines Schutzmechanismus beeinflusst die Proaktivität, die Trefferquote erkannter Viren und erfordert auch die Mitwirkung des Nutzers.

- ▶ **Proaktivität:** Sie beschreibt die Fähigkeit der Sicherheitslösung, neue beziehungsweise noch nicht von Antiviren-Laboren klassifizierte Schädlinge zu entdecken. Einfache Analyseverfahren wie der Signaturvergleich können nur bekannte Schadprogramme entdecken. Je komplexer das analytische System, desto höher ist auch seine Proaktivität. Letztere hängt aber auch entscheidend davon ab, wie häufig das Antiviren-Programm seine Malware-Datenbank aktualisiert. Beispielsweise müssen Signaturdatenbanken oft erneuert werden, während Expertensysteme auch monatelang ohne Update zuverlässig funktionieren.
- ▶ **Trefferquote:** Je komplizierter die Analysetechnologie, desto mehr Schädlinge lassen sich damit auch entdecken. Signaturbasierte Methoden sind hier im Nachteil, da sie wesentlich unflexibler agieren als Systeme, die Malware verhaltensbestimmt aufspüren.
- ▶ **Mitwirkung:** Ohne Unterstützung des Anwenders arbeitet ein Antiviren-Programm nicht zuverlässig. Je weiter die Viren-Analyse von einem primitiven Vergleich entfernt ist, desto öfter gibt es falschen Alarm, der manuell korrigiert werden muss. Dazu braucht es unbedingt die Mitwirkung des Nutzers. Dieser sollte auch Regeln und Ausnahmefälle definieren sowie Programme auf Black- und Whitelists setzen können.

Kennt man die Vorzüge und Nachteile von Antiviren-Verfahren, lassen sie sich auch leichter bewerten. So gewährt zum Beispiel ein Emulator mit komplizierter analytischer Komponente einen sicheren Schutz, weil

zu überprüfende Dateien nicht ausgeführt werden müssen. Gegen einen gewissen Prozentsatz an Schadprogrammen ist dieses System jedoch wirkungslos – sei es durch Sicherheitslücken im Emulator oder aufgrund neuartiger Schadprogramme. Insgesamt wird ein solcher Schutz zwar einen hohen Anteil unbekannter Malware identifizieren, arbeitet jedoch zwangsläufig langsam.

### Die passende Antiviren-Lösung

Die meisten Antiviren-Programme setzen eine Signaturerkennung ein und kombinieren sie entweder mit einer Systemüberwachung, einem Emulator oder verwenden eine Sandbox. Doch für welche Variante soll sich der Anwender entscheiden?

Eine universelle Lösung gibt es leider nicht. Jede Technologie hat spezielle Vor- und Nachteile. Beispielsweise beansprucht die Systemüberwachung ständig Prozessorzeit, kann dafür aber von den meisten Schadprogrammen nicht überwunden werden. Ein Emulationsprozess lässt sich mit bestimmten Befehlen überlisten, dafür bleibt das Betriebssystem beim Malware-Scan unangetastet. Und noch ein Beispiel: Systeme mit einfachen Regeln melden sich mit vielen Rückfragen beim Nutzer. Kompliziertere Lösungen benötigen dagegen weniger Feedback, verursachen aber den einen oder anderen falschen Alarm.

Wer einen leistungsstarken Rechner verwendet und sich sehr um die Sicherheit seiner Daten sorgt, sollte eine Antiviren-Lösung mit Sandbox einsetzen. Ein solches System bietet maximale Sicherheit, fordert aber viele Systemressourcen und kann das Arbeiten daher verlangsamen.

Für den Spezialisten, der kritische Systemereignisse kontrollieren und unbekannte Schadprogramme abwehren will, empfiehlt sich eine Echtzeit-Systemüberwachung. Diese belastet den Rechner gleichmäßig, bremst ihn aber nicht so stark aus wie eine Sandbox. Dafür lässt sich die Systemüberwachung bis ins Detail manuell konfigurieren. Anwender, die ihren PC weder mit einer Systemüberwachung belasten noch Regeln selbst aufstellen wollen, genügt dagegen auch eine einfachere Heuristik-Lösung.

Systeme, die mit nicht signaturbasierten Verfahren arbeiten, teilen sich in zwei Kategorien. Zur ersten zählen HIPS-Systeme wie Prevx oder Cyberhawk, die sich aber auf einen kleinen Bereich spezialisiert haben. Die zweite Kategorie umfasst Antiviren-Programme, die im Zuge ihrer Entwicklung nun auch nicht-signaturbasierte Verfahren einsetzen und zahlreiche Malware-Programme abwehren können.

Welches Produkt man einsetzt, entscheidet letztlich der persönliche Eindruck. Unabhängige Tests helfen bei der Auswahl.

**Alisa Shevchenko**  
Viren-Analystin, Kaspersky Lab

### Weblinks

Unabhängige Tests von Antiviren-Software:

- AV-Comparatives  
[www.av-comparatives.org](http://www.av-comparatives.org)
- West Coast Labs (Checkmark Certification)  
[www.westcoastlabs.com/checkmark](http://www.westcoastlabs.com/checkmark)
- AV-Test  
[www.av-test.org](http://www.av-test.org)
- ICSA Labs  
[www.icsalabs.com](http://www.icsalabs.com)
- Virus Bulletin  
[www.virusbtn.com](http://www.virusbtn.com)
- Anti-Malware  
[www.anti-malware-test.com](http://www.anti-malware-test.com)

Unabhängige Tests von HIPS-Systemen:

- Tech Support Alert  
[www.techsupportalert.com/security\\_HIPS.htm](http://www.techsupportalert.com/security_HIPS.htm)
- Lycos  
[http://membres.lycos.fr/nicmtests/Unhookers/unhooking\\_tests.htm](http://membres.lycos.fr/nicmtests/Unhookers/unhooking_tests.htm)
- AV-Comparatives  
[www.av-comparatives.org/seiten/ergebnisse/HIPS-BB-SB.pdf](http://www.av-comparatives.org/seiten/ergebnisse/HIPS-BB-SB.pdf)

## Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crime-ware, Hacker, Phishing-Attacken und Spam.

Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht.

Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

### Kontakt

Kaspersky Labs GmbH  
Steinheilstr. 13  
85053 Ingolstadt

Telefon: +49 (0)841 981 89 0  
Telefax: +49 (0)841 981 89 100

info@kaspersky.de  
www.kaspersky.de