

Warum herkömmliche Sicherheitssoftware nicht mehr ausreichend schützt

**Ein Überblick über die aktuelle Bedrohungslandschaft
und wie AVG 9.0 Sie und Ihr Unternehmen online
zuverlässig schützen kann**

Inhalt

Warum diese Informationen für PC-Nutzer wichtig sind	3
Die Entwicklung von kommerziellen Schadprogrammen	4
Die digitale Identität – eine wertvolle Ware in der Schattenwirtschaft	5
Lug und Trug im World Wide Web.....	5
Warum aktuelle Sicherheitssoftware häufig nicht ausreicht	6
Die drei Schutzebenen von AVG.....	8
Warum die dritte Schutzebene heute entscheidend ist.....	10
Die Kombination aus Firewall, Identitätsschutz und Resident Shield	11
AVG Cloud Services	11
AVG 9.0: Rundum Gut Geschützt	12
Für den privaten Gebrauch	12
Für den gewerblichen Gebrauch	13
Über AVG Technologies	14
AVG im World Wide Web.....	14
Referenzen.....	15

Warum diese Informationen für PC-Nutzer wichtig sind

Computersicherheit war einmal eine einfache Angelegenheit. E-Mails waren meist das Mittel der Wahl, um ein fremdes Computersystem zu kompromittieren. Wer über ein Anti-Virus-Programm verfügte und Vorsicht beim Öffnen von Dateianhängen walten ließ, brauchte sich um die Sicherheit seines Rechners kaum zu sorgen. Denn die Konsequenzen für ein infiziertes System hielten sich in Grenzen: Technische Schwierigkeiten oder Datenverlust waren die wahrscheinlichste Folge. Doch die Zeiten haben sich geändert. Das Internet ist zum Hauptangriffsweg von Cyberkriminellen geworden. Vor allem Profitgier treibt die Online-Kriminellen an, ständig neue und immer weiter ausgeklügelte Bedrohungen zu entwickeln und zu verbreiten.

Dieser Bericht enthält einen Überblick über die aktuelle Gefahrenlage im World Wide Web. Er zeigt auf, warum herkömmliche Security-Lösungen nicht mehr ausreichen und wie AVG 9.0 vorhandene Sicherheitslücken schließen kann.

Die Entwicklung von kommerziellen Schadprogrammen

Vor zehn Jahren entwickelten hauptsächlich junge und ambitionierte Amateur-Programmierer – sogenannte script kiddies oder script bunnies – Viren und andere Formen von Malware. Sie wollten andere durch technisches Know-how beeindrucken und einen gewissen Bekanntheitsgrad in der Hackerszene erlangen. Es ging ihnen schlicht darum, PC-Nutzern mit Schadsoftware Unannehmlichkeiten zu bereiten. Sie brachten etwa die Daten der Anwender durcheinander oder beeinträchtigten die Stabilität der Rechner. Nur einige wenige Schadprogramme führten zu schweren Systemzusammenbrüchen, der Großteil war relativ einfach konstruiert sowie leicht zu erkennen und zu blockieren.

In den letzten Jahren hat sich die Sicherheitslandschaft allerdings merklich verändert. Organisierte kriminelle Banden haben entdeckt, dass sich mit Malware viel Geld machen lässt. Sie rekrutieren erfahrene Programmierer, um schädliche Software zum Diebstahl von Geld und persönlichen Daten zu entwickeln. Eine ganze Wirtschaftbranche lebt heute von dem Geschäft mit unsicheren PCs. Kriminelle bieten nicht nur gestohlene Daten zum Kauf an, sondern auch die jeweiligen Programme, mit denen sich vertrauliche Informationen ausspionieren lassen. Ganze Selbstbaukästen, wie zum Beispiel MPack¹, veräußern sie als kommerzielle Malware, einschließlich Support und Update-Möglichkeiten. Dadurch sind auch Personen ohne Programmierkenntnisse in der Lage, ausgeklügelte Angriffe gegen ahnungslose Nutzer zu starten. Sowohl die Häufigkeit der Betrugsversuche als auch die Anzahl der kompromittierten Systeme ist durch diese Entwicklung im Laufe der Jahre exponentiell angestiegen. Allein 2008 wurden mehr als 1,5 Millionen neue Malware-Stämme identifiziert – jeden Tag erreichen Zehntausende von neuen Exemplaren die Forschungslabore der Sicherheitsfirmen.

Die heutigen Sicherheitsbedrohungen sind immer komplexer und stärker miteinander vernetzt. Diente zum Beispiel das Verschicken von Spam früher dazu, kleine blaue Viagra-Pillen oder gefälschte Software an den Mann zu bringen, lassen sich heute mit den ungebetenen Mails unter anderem gefährliche Würmer verbreiten. Zum Beispiel wurden Rechner, die sich mit dem Storm-Wurm² infiziert hatten, in ein ferngesteuertes Netzwerk von Computern eingebunden, ein sogenanntes *Botnet*. Dieses zentral kontrollierte Netzwerk bestand aus bis zu 50 Millionen Rechnern, die dazu missbraucht wurden, Spam zu verschicken und den Wurm weiter zu verbreiten - natürlich ohne Wissen der Computerbesitzer. Das Netzwerk erweiterte sich dadurch kontinuierlich. Zusätzlich konnten Kriminelle Rechenzeit im Botnet buchen, um darüber eigene betrügerische E-Mails zu versenden. Zwar ist das Storm-Botnet voraussichtlich ausgestorben, aber andere Bedrohungen, wie zum Beispiel Conficker³, nehmen inzwischen auf der Bildfläche dessen Platz ein.

Die digitale Identität – eine wertvolle Ware in der Schattenwirtschaft

Für Millionen von Menschen gehören finanzielle Transaktionen über den Computer genauso zum Alltag wie das tägliche Zähneputzen. Die Anwender speichern auf dem PC daher eine große Anzahl von persönlichen Informationen und übertragen sie etwa beim Online-Banking, Shopping oder Buchen einer Reise im Internet. Das macht private und geschäftlich genutzte Rechner extrem attraktiv als Angriffsziel für Kriminelle. Ist ein Computer erstmal kompromittiert, ist es für Kriminellen häufig ein Leichtes, die Kommunikation abzufangen und sensible Daten auszuspionieren, wie zum Beispiel:

- Geburtsdaten
- Versicherungsnummern oder Nummern von Ausweisdokumenten
- Online-Banking-Informationen incl. Zugangskennwörter
- E-Mail-Adressen und Passwörter
- Anschriften
- Telefonnummern
- Details zum Beschäftigungsverhältnis

Mit anderen Worten: Kriminelle können über einen ungeschützten Rechner wichtige, persönliche Daten abziehen und mit dieser gestohlenen Identität im Internet ihr Unwesen treiben.

Auf dem Missbrauch dieser Daten beruht eine Multi-Milliarden Euro-Industrie. Laut einer Studie von Javelin Strategy and Research⁴ haben im Jahr 2008 knapp zehn Millionen US-Bürger insgesamt 48 Milliarden Dollar durch Identitätsbetrug verloren. Gartner, ein führendes Forschungs- und Beratungsunternehmen, beziffert allein den durch Phishing-Betrug im Jahr 2007 entstandenen Schaden auf mehr als dreieinhalb Milliarden Dollar.

"Die Angriffe auf Browser aus dem Web zielen vermehrt auf einzelne Komponenten wie Flash oder Quicktime ab, die nicht automatisch einen Sicherheitspatch erhalten, wenn der Browser ein Update bekommt. Gleichzeitig haben sich Angriffe von Webseiten weiter entwickelt – von einfachen 'Exploits', über Skript-basierte Angriffe, die mehrere Schwachstellen ausnutzen bis hin zu ausgeklügelten Systemen, die wie der Wolf im Schafspelz ihre wahren Absichten mit ganzen Modulen tarnen. Eines der aktuellen Module – MPack – brüstet sich mit einer Erfolgsquote von 10%-25% beim Auffinden und Ausnutzen von Browser-Schwachstellen, sobald ein Browser eine mit dem Modul infizierte Webseite besucht. Währenddessen platzieren Angreifer ihren Angriffscode auf bekannten und für die Nutzer scheinbar vertrauenswürdigen Websites. Je besser sie Angriffswerkzeuge auf vertrauenswürdigen Seiten unterbringen, desto größer ist der Vorteil für die Angreifer gegenüber der nichtsahnenden Öffentlichkeit."

SANS Institute, Top Ten Cyber Menaces for 2008⁶

Lug und Trug im World Wide Web

Das kriminelle Potenzial von Hackern richtet sich heute vollständig auf das Web. Per E-Mail haben Angreifer zwar immer noch die Möglichkeit, Computer zu bedrohen – etwa durch infizierte Anhänge oder einen Link zu einer Webseite, die mit Schadcode präpariert ist. Doch hat sich mit der Entstehung des sogenannten Web 2.0 die mögliche Angriffsfläche für Cyberkriminelle spektakulär erweitert. Im sogenannten Social Web ergeben sich immer neue Wege, Systeme zu infizieren, zum Beispiel mit Mechanismen wie Cross-Site-Scripting in AJAX und RSS/Atom. Auch Sicherheitslücken in Web-Browsern und Browser Add-Ons, wie zum Beispiel Flash, QuickTime oder Microsoft Silverlight, sind immer wieder ein Einfallstor für Kriminelle. Über sie können ganz unterschiedlichen Arten von Malware in das System eindringen, etwa Keylogger oder Trojaner, die es auf Passwörter abgesehen haben. Allein beim Browser Internet Explorer wurden in den vergangenen zwei Jahren über 75 Sicherheitslücken bekannt. Ganz aktuell erobern die Angreifer neues Terrain mit manipulierten Seiten in Sozialen Netzwerken.

Die Schlussfolgerung: Keine Homepage ist zu 100 Prozent sicher – selbst seriöse und vertrauenswürdige Seiten können kompromittiert sein. So verbreitet sich Malware ohne das Wissen des Seitenbetreibers weiter. Eine beliebte Methode in Hackerkreisen ist es zum Beispiel, über Werbebanner Sicherheitslücken in Web-Browsern und Browser-Add-Ons auszunutzen. Über die angeschlossenen Werbenetzwerke verteilt sich die Schadware in diesen Fällen schnell auf unzähligen Webseiten. Studien machen das Ausmaß deutlich: Im zweiten Halbjahr 2008 waren 70 der 100 weltweit meist besuchten Webseiten entweder infiziert oder enthielten Links zu anderen gefährlichen Sites.⁷ Im Januar 2009 belief sich die Anzahl der infizierten Homepages auf mehrere Tausend. Auch Seiten von börsennotierten Unternehmen, Bundesämtern, Botschaften, Stars und sogar von Sicherheitsfirmen wurden benutzt, um persönliche Daten von ahnungslosen Besuchern abzugreifen⁸.

Warum aktuelle Sicherheitssoftware häufig nicht ausreicht

"Das Credo der heutigen Web-Infektionen lautet: Heute hier, morgen da. Im Gegensatz zum AVG LinkScanner verlassen sich manche Web Security-Produkte lediglich darauf, regelmäßig Webseiten zu besuchen, auf Bedrohungen zu prüfen und das Ergebnis dann als Sicherheitseinstufung abzuspeichern. Das ist viel zu wenig, denn sie müssten jeden Tag Hunderte Millionen von Webseiten überprüfen, um einigermaßen adäquaten Schutz zu liefern. Selbst mit heutigen Supercomputern wäre das technisch jedoch nicht machbar."

J.R.Smith, Vorstandsvorsitzender von AVG Technologies

Um erfolgreich Daten oder Geld zu stehlen, versuchen Online-Gangster ihre Schadprogramme möglichst lange auf dem Rechner zu verstecken. Neue Malware-Varianten sind folglich immer besser getarnt als bereits bekannte Angriffsformen. Allein das Besuchen einer vermeintlich sicheren Homepage kann heute ein Risiko darstellen. Ohne das Wissen des Nutzers bedient sich die schädliche Software an sensiblen, persönlichen Informationen. Oft ist der Schaden bereits erheblich, wenn ein Anwender den Eindringling bemerkt, und herausfindet, dass sein Online-Account kompromittiert ist oder seine Kreditkartenabrechnung unerklärliche Abbuchungen enthält. Wie erfolgreich Cyber-Kriminelle mit ihren Angriffen sind, kann daher nicht allein von der Wachsamkeit der PC-Benutzer abhängen. Vielmehr sind zuverlässige Sicherheitsprodukte gefragt, die mit immer weiter entwickelten Technologien den Angreifern Einhalt gebieten.

So scannen zum Beispiel Suchmaschinen wie Google und Webschutz-Produkte wie Site Advisor oder Phishing-Filter das Web, um gefährliche Inhalte aufzufinden und auf eine schwarze Liste zu setzen, die sogenannte Blacklist. Um sich vor diesen Tools bestmöglich zu verstecken, greifen Online-Kriminelle neuerdings verstärkt auf temporäre, manipulierte Webseiten zurück, die nur wenige Stunden online sind. Nach dem Abschalten der einen Homepage veröffentlichen die Angreifer den gefährlichen Inhalt einfach auf einer neuen Seite. Untersuchungen von AVG zeigen, dass über 200.000 infizierte neue Webseiten jeden Tag online gehen. Davon sind mehr als die Hälfte weniger als 24 Stunden im Netz. Trotzdem gelingt es, in dieser kurzen Zeit eine beträchtliche Anzahl von Computern zu infizieren – etwa durch Spam-Kampagnen die via eines Botnetzes oder Social-Networking-Seiten wie Facebook verbreitet werden.

Herkömmliche Antivirus-Software arbeitet mit sogenannten *Signatures*, um Malware zu entdecken. Es handelt sich dabei um Byte-Sequenzen beziehungsweise Codeausschnitte aus den originalen Schadprogrammen. Sobald die Sicherheitslabore der Softwarehersteller neue Ausschnitte einer Malware identifizieren, stellen sie diese Information über ein Programm-Update allen Anwendern der Software zur Verfügung. Der PC des Anwenders kann nun anhand der Signaturen musterbasiert suchen. Das Programm fahndet nach Dateien mit Codeausschnitten, die mit den Malware-Informationen aus der Datenbank übereinstimmen. Ist die Suche erfolgreich, klassifiziert das Programm die gefundene Datei als Malware und benachrichtigt den Anwender. So gelingt es den Schädling zu blockieren oder zu entfernen, bevor ein Schaden entsteht.

Damit Malware länger unentdeckt bleibt und somit mehr Rechner infizieren kann, setzen Cyber-Kriminelle alles daran, ihre Schadprogramme vor den Forschungslaboren der Sicherheitssoftware-Hersteller zu verbergen: Denn ohne Malware-Samples keine Signaturen. Zu diesem Zweck bedienen sie sich einer Vielfalt an Techniken: Angefangen von Browser- und Betriebssystemüberprüfungen, über Download-Obergrenzen bis hin zu Zufallsverfahren. So gelingt es, jedem Besucher beim Aufrufen der Website unterschiedliche Inhalte zu präsentieren. Die automatischen Suchprogramme der Sicherheitsunternehmen sehen einen komplett harmlosen Code, während Besucher mit kritischen Sicherheitslücken im Browser den gefährlichen Inhalt aufrufen.

Doch sogar wenn Hersteller von Sicherheitssoftware das Sample eines Schadprogramms besitzen, können sie es nicht automatisch abwehren. Das Blockieren ist heute deutlich schwieriger als früher. Denn mit selbstverändernden¹⁰ und polymorphen¹¹ Programmieretechniken kann die Malware nach jeder neuen Infektion ihre Signaturen verändern. Auch sind Schadprogramme häufig verschlüsselt, damit Anti-Virus-Scanner sie nicht aufspüren können. Darauf reagieren wiederum die Software-Hersteller. Die Sicherheitsprogramme sollen in diesem Fall nicht den Virus selbst, sondern die jeweilige Verschlüsselungstechnik erkennen. Fast könnte man von einem Katz-und-Maus-Spiel sprechen, das technisch schwer zu gewinnen ist.

Eins steht jedoch fest: Moderne Malware ist anspruchsvoller geworden und verändert sich extrem schnell. Vor allem enthüllt sie die Mängel der herkömmlichen Sicherheitsmethoden, die auf dem Signatur-Prinzip basieren. Damit steigt die Bedrohung für all jene Nutzer, die sich auf klassische Antivirenprogramme verlassen. Untersuchungen einer Sicherheitsfirma aus dem Jahr 2007 verdeutlichen das Ausmaß des Problems: 72 Prozent der nur mit signaturbasierten Sicherheitslösungen geschützten Unternehmensrechner und 23 Prozent der Heimcomputer mit herkömmlicher AV-Software wurden mit Malware infiziert. Forschungsergebnisse von Core Trace im Sommer 2009 ergaben, dass mehr als 50 Prozent der Unternehmen eine signaturbasierte Sicherheitssoftware für unzureichend halten, um aktuellen Bedrohungen zu begegnen.

Die drei Schutzebenen von AVG

Die AVG Sicherheitsprodukte schirmen den Rechner auf drei Ebenen vor Angriffen ab. Jede von ihnen enthält eine besondere Schutzfunktion. Sie ergänzen sich gegenseitig und ergeben somit ein optimales Sicherheitsniveau. Bildlich gesprochen kann man den Rechner mit einem Datenträger vergleichen, auf dem sensible, persönliche Daten gespeichert sind. Wie Scheiben eines Schweizer Käse legen sich die drei Schutzebenen über den Datenträger, um Schädlinge verschiedener Art abzuwehren. Dabei bilden die Löcher in den Käsescheiben mögliche Angriffsflächen für Malware. Erst wenn drei Käsescheiben übereinanderliegen, werden die jeweiligen Löcher von den anderen Scheiben überdeckt und kein Angreifer dringt mehr zu den persönlichen Daten durch.

Die erste Schutzebene von AVG enthält den traditionellen Anti-Virus-Schutz. Er entdeckt und blockiert bereits bekannte Viren, Würmer und Spyware durch den Abgleich mit einer Datenbank. Dieser signaturbasierte Scanner wurde in AVG 9.0 deutlich verbessert. In einem allerersten Scandurchlauf kennzeichnet er alle Dateien als sicher oder potentiell gefährlich. Bei zukünftigen Scans überspringt er die sicheren Dateien so lange, bis sich die Dateiablagestruktur verändert. Dies ermöglicht eine drastische Reduzierung der Scanzeit um bis zu 50 Prozent, abhängig von der jeweiligen Systemkonfiguration. Parallel gehen sowohl die Bootzeiten als auch der Speicherverbrauch um zehn bis 15 Prozent zurück. Doch funktioniert dieses Prinzip nur bei bekannten Gefahren. Grund dafür sind die bereits erwähnten Signaturen. Da von unbekanntem Schadprogrammen keine Codeausschnitte existieren, kann auch kein Vergleich mit der Datenbank des Sicherheitsprodukts stattfinden. Unbekannte Viren und kurzlebige Webbedrohungen lassen sich mit einem herkömmlichen Anti-Viren-Scanner daher nicht aufspüren. Wie Luft die Löcher des Käse durchdringen, so passieren unbekannte Schädlinge die Sicherheitslücken dieser ersten Schutzebene.

Der AVG LinkScanner mit den Technologien Safe Surfing und Safe Searching bildet die zweite Schutzebene der AVG Sicherheitsprodukte. Brandneue Bedrohungen im Web, die am nächsten Tag schon wieder verschwunden sein können, wehrt das Tool zuverlässig ab. LinkScanner erkennt die Gefahren, die sich auf einer Webseite verbergen können und blockiert sie zuverlässig. Dazu nimmt der Webschutz eine Sicherheitsüberprüfung in Echtzeit vor, da heißt, er untersucht die Webseiten genau in dem Moment, in dem ein Anwender ein Web-Angebot aufruft.

Andere Programme teilen dem Nutzer nur mit, ob die Webseite zum Zeitpunkt der letzten Überprüfung sicher war – was Wochen oder sogar Monate zurückliegen kann. Da über 60 Prozent der gefährlichen Inhalte nicht einmal 24 Stunden auf der gleichen Webseite verweilen, sind derartige Informationen für den Anwender nur wenig hilfreich.

In der Version 9.0 wurde der AVG LinkScanner um einen verbesserten Anti-Phishing Schutz ergänzt. Er ermöglicht das schnellere und gezieltere Aufdecken von Phishing-Attacken auf einer Website. Dazu durchleuchtet der LinkScanner die aufgerufene Homepage zunächst auf über 100 verschiedene und potentielle Bedrohungsindikatoren. Reicht dies nicht für eine zuverlässige Entscheidung aus, greift die Komponente auf die AVG Cloud-Services zurück, die zahlreiche Nachrichtenquellen zum Thema Betrugsschutz zusammenführen. Anschließend fällt er ein eindeutiges Urteil bezüglich des Bedrohungspotentials.

Viele Sicherheitslücken sind nun schon eliminiert.

Die dritte und letzte Schutzebene ist das Besondere in AVG 9.0. Sie schützt sensible Daten vor allen neuen und bisher unbekanntem Bedrohungen. Dazu arbeiten die Komponenten Resident Shield, Firewall und Identitätsschutz im Team, das heißt sie sind in der Lage, Informationen über Malware untereinander auszutauschen. Schadprogramme, für die noch keine Signaturen entwickelt wurden, kann AVG 9.0 dadurch noch besser erkennen und entfernen.

Dies gelingt durch die Kombination verschiedener, innovativer Methoden: Verhaltensbasierte Sicherheit, Cloud Security und Whitelisting ergänzen sich gegenseitig und sorgen für ein Höchstmaß an Schutz.

Legt man die drei Schutzebenen übereinander, sind alle Sicherheitslücken geschlossen und kein Schädling dringt mehr zu den persönlichen Daten auf dem Rechner durch.

Doch wie genau funktioniert der Schutz, der nicht auf herkömmlichen Virensignaturen basiert?

Der verhaltensbasierte Schutz in AVG Internet Security ist in der Lage, Malware anhand charakteristischer Verhaltensmuster zu identifizieren. Dieser Prozess nennt sich heuristische Erkennung oder heuristische Analyse. Man kennt das Vorgehen aus dem täglichen Leben: Was aussieht wie ein Fahrrad, fährt wie ein Fahrrad und auch noch klingelt wie ein Fahrrad – ist vermutlich ein Fahrrad. Als Mensch führt man diese Erkennung innerhalb von Sekundenbruchteilen durch. Selbst wenn nicht alle Informationen gleich bereit stehen erkennt man das Objekt sofort.

Die heuristische Analyse geht ganz ähnlich vor: Um an persönliche Nutzerdaten zu gelangen, führt Schadsoftware bestimmte Aktionen auf dem Rechner aus, die vertrauenswürdige Software normalerweise nicht vollführt. Ein seriöses Programm versucht zum Beispiel nicht, seine Anwesenheit auf einem Rechner zu verschleiern, Quelltext in andere Programme einzuschleusen, Tastatureingaben abzufangen oder auf Bereiche des PCs zuzugreifen, in denen Passwörter abgelegt sind. Verhaltenserkennung spürt derartige Unregelmäßigkeiten auf, identifiziert die potentielle Malware und blockiert sie, bevor ein Schaden entsteht.

Der große Vorteil: Das Zeitfenster ohne Schutz – nämlich zwischen der Verbreitung einer Malware bis zur Veröffentlichung der entsprechenden Signatur durch die Antivirus-Hersteller - fällt vollständig weg. Der Schutz greift sofort, ohne zeitliche Verzögerung. Im Gegensatz zu Virensignaturen erkennen Sicherheitsprogramme mit Verhaltenserkennung daher auch bisher unbekannte Schadware.

Genau so wie der Mensch funktioniert das Modul AVG Identitätsschutz auf der Basis von Erfahrungswerten. Die Verhaltensanalyse untersucht die Kommunikation und Interaktion zwischen den Programmen auf dem PC. Sie entdeckt, analysiert und deaktiviert verdächtige Aktivitäten auf dem Rechner, bevor Malware Schaden anrichten kann. Dieser Prozess läuft in Echtzeit im Hintergrund ab, ohne die System-Performance merklich zu beeinflussen.

Der verhaltensbasierte Identitätsschutz von AVG bringt eine Reihe von Vorteilen:

- Das Modul schützt vor dem Diebstahl persönlicher Daten und entdeckt und blockiert anhand typischer Verhaltensweisen auch völlig neue und bisher unbekanntem Bedrohungen, wie zum Beispiel Rootkits, Trojaner oder Keylogger.
- Die Verhaltensanalyse bildet eine zusätzliche proaktive Schutzebene, die kontinuierlich und selbständig agiert und dafür keine Scanengine oder Signaturen benötigt.
- Die Fehlalarmquote ist im Schnitt zehnmal geringer als bei anderen verhaltensbasierten Produkten.

Darüber hinaus ist AVG Identitätsschutz in der Lage, die Fremdsteuerung eines Systems durch Hacker zu unterbinden, bevor ein Schaden entsteht. Dadurch lassen sich deutlich mehr Angriffe aufdecken. Auch Malware die sich selbst kopiert und auf dem Rechner ausbreitet, erkennt und entfernt der verhaltensbasierte Schutz.

Ebenso wie der AVG LinkScanner ist das Modul AVG Identitätsschutz als Einzelprodukt erhältlich und zur Verbesserung der Schutzfunktion üblicher Antivirus- und Anti-Malware-Programme einsetzbar. Es müssen keine weiteren AVG Sicherheitslösungen auf dem Rechner installiert sein. Allerdings garantiert die Kombination der Produkte ein bestmögliches Sicherheitsniveau, da die verschiedenen Schutzebenen aufeinander abgestimmt sind und sich gegenseitig ergänzen.

Warum die dritte Schutzebene heute entscheidend ist

Einzel betrachtet bietet keines der oben beschriebenen Sicherheitsverfahren vollständigen Schutz: Sowohl signaturbasierte als auch heuristische oder verhaltensbasierte Produkte allein sind für bestimmte Angriffsformen durchlässig. Erst die Kombination aller Sicherheitsmechanismen reduziert das Risiko einer Malware-Attacke drastisch.

Hinzu kommt, dass neue Gefahren im Netz häufig sehr kurzfristig auftauchen und verschwinden. Jeden Tag werden rund zwei Millionen neue Webseiten mit versteckten Angriffen infiziert. 60 Prozent dieser Bedrohungen verschwinden jedoch innerhalb eines Tages wieder oder treten an einem anderen Ort auf. Um vor diesen schnelllebigen Schädlingen zu schützen, nutzt AVG 9.0 das ganze Spektrum an innovativen Methoden: Signatur- und verhaltensbasierte Sicherheit, Cloud Security und Whitelisting kommen zum Einsatz, um der Vielzahl an Bedrohungen Herr zu werden, die im World Wide Web täglich neu entstehen. Zusammengeführt werden die Methoden durch die Kooperation der Komponenten Resident Shield, Firewall und Identitätsschutz. Sie tauschen Malware-Informationen untereinander aus und sind daher in der Lage, Bedrohungen zu erkennen und zu entfernen, für die noch keine Virensignaturen existieren.

Und so funktioniert der Schutz im Einzelnen:

Die Firewall wurde in AVG 9.0 komplett neu entwickelt und macht sich die Methode des Application Whitelisting zu nutze. Dadurch reduzieren sich die Fehlalarmmeldungen um 50 Prozent. Die neue Firewall kommuniziert dazu im Hintergrund mit dem verhaltensbasierten Identitätsschutz, was die Erkennung von neuen und unbekanntem Bedrohungen besonders exakt macht. Nach Einschätzungen von AVG sind die Fehlermeldungen sogar um 90 Prozent geringer als in anderen, vergleichbaren Produkten, die mit ähnlichen Verfahren arbeiten.

Das höhere Schutzniveau in AVG 9.0 erweist sich auch als sehr effektiv gegen jede Form von Phishing-Attacken. Sobald das System eindeutige Anzeichen einer neuen Bedrohung erkennt, greift die Sicherheitssoftware auf die AVG Cloud-Services zurück. Sie führen zahlreiche Nachrichtenquellen zum Thema Betrugsschutz zusammen, um zu einer realistischen Gefahreinschätzung zu gelangen. Denn auch hier gilt: Je früher die Software eine Bedrohung aufspürt, desto besser ist der PC-Nutzer geschützt.

Die Kombination aus Firewall, Identitätsschutz und Resident Shield

Jede Sicherheitskomponente in AVG 9.0 nutzt eigene Technologien, um mögliche neue Gefahren aufzuspüren. Kombiniert man die so gewonnenen Informationen miteinander, erhält man einen allumfassenden Schutz. Der folgende Absatz erklärt, wie die Module interagieren und welche Vorteile für AVG 9.0 daraus resultieren:

Firewall und Identitätsschutz

Sobald die Firewall registriert, dass eine Anwendung oder ein Dienst eine Verbindung ins Internet herstellen möchte, konsultiert sie das Modul AVG Identitätsschutz. Stuft diese verhaltensbasierte Komponente die Verbindung als vertrauenswürdig ein, reicht sie diese Information an die Firewall weiter. Der PC-Nutzer muss somit nicht auf ein Dialogfenster reagieren. Stellt der Identitätsschutz allerdings fest, dass die Anfrage gefährlich ist, dann instruiert er die Firewall, alle Kommunikationskanäle zu kappen. Diese Vorgehensweise verhindert, dass persönliche Daten den Rechner verlassen, bevor die Bedrohung überhaupt erkannt ist. Führt im Gegenzug das Modul Identitätsschutz eine verhaltensbasierte Analyse aus, tauscht es ebenfalls Informationen mit der Firewall aus – allerdings auf umgekehrtem Dienstweg.

Resident Shield und Identitätsschutz

Wenn die Komponente Resident Shield registriert, dass eine gefährliche Datei auf dem Rechner installiert werden soll, leitet sie diese Information an den verhaltensbasierten Identitätsschutz weiter. Dieser überprüft, ob einzelne Dateikomponenten, die das Resident Shield möglicherweise nicht entdeckt hat, eine Gefahr darstellen. Ist dies der Fall, entfernt er sie. Allein die Ähnlichkeit mit dem System bekannter Malware, gibt hier den Ausschlag für die Entscheidung.

AVG Cloud Services

Der AVG LinkScanner überprüft beim Aufrufen einer Website zunächst über 100 verschiedene Bedrohungsindikatoren. Reicht dies für eine zuverlässige Entscheidung nicht aus, greift die Komponente auf die AVG Cloud-Services zurück, die zahlreiche Nachrichtenquellen zum Thema Betrugsschutz zusammenführen. Dieser Service gibt an, ob es sich um einen sicheren, gefährlichen oder unbekanntem Prozess handelt. Bei sicheren oder unsicheren Prozessen werden entsprechende Maßnahmen eingeleitet. Falls ein Prozess unbekannt ist, führt der Rechner ihn solange aus bis genügend verdächtige Aktivitäten dokumentiert sind. Die Sicherheitslösung beobachtet sämtliche Aktivitäten. Um das Risiko abschließend festzustellen, wird der Prozess mit der Zustimmung des Nutzers zusätzlichen Analysen unterzogen. AVG 9.0 leitet das Ergebnis der Untersuchungen schließlich an den AVG Cloud Service weiter. Alle AVG-Anwender, die beim Surfen auf die gleiche Bedrohung treffen, können nun unmittelbar mit den einmal in der Cloud analysierten Informationen versorgt werden. Diese Vorgehensweise verhindert, dass Malware großen Schaden anrichten kann und vermeidet Fehlalarme. Die Information wird der internen Konfiguration hinzugefügt und alle Agenten erhalten anschließend ein Konfigurations-Update.

AVG 9.0: Rundum Gut Geschützt

Für den privaten Gebrauch

AVG Internet Security

Umfassender Schutz – inklusive LinkScanner-Technologie und AVG Identitätsschutz

Ob beim Surfen, Shoppen, Online-Banking, Dateien downloaden oder Chatten mit Freunden: Mit AVG Internet Security sind Sie rundum gut geschützt. Das Sicherheitspaket sichert Ihre persönlichen Daten vor bekannten und unbekanntem Gefahren, egal ob Sie online oder offline sind. Die drei Schutzebenen in AVG Internet Security verhindern unautorisierten Zugriff auf sensible Informationen und schützen Ihren PC selbst vor den neuesten, sehr ausgeklügelten Bedrohungen. Anwender erhalten kostenlosen Online-Support, überall auf der Welt, rund um die Uhr.

AVG Anti-Virus

Effizienter Viren- und Spyware-Schutz – die Basis für sichere Online-Aktivitäten

AVG Anti-Virus schützt vor Viren, Würmern und Trojanern und verhindert deren unbewusste Weitergabe. Die Software enthält AVG LinkScanner, der wirkungsvoll vor dem ungewollten Besuch schadhafter Webseiten schützt. Das Tool prüft Links und Web-Inhalte in Echtzeit, also genau in dem Moment, in dem sie aufgerufen werden.

AVG Identitätsschutz

Ständig aktualisierter Schutz für Online-Banking und -Shopping

Je mehr Zeit Sie im Internet verbringen, desto wichtiger ist es, persönliche Daten vor Identitätsdiebstahl zu schützen. AVG Identitätsschutz legt sich über Ihre vorhandene Antivirenlösung und sichert Ihre Kennwörter, Kreditkarteninformationen und andere digitale Daten vor Beobachtern. AVG Identitätsschutz erweitert nicht nur Produkte von AVG, sondern jede auf dem Markt erhältliche Antivirenlösung.

Kostenlosen Basisschutz bieten darüber hinaus AVG Anti-Virus 9.0 Free Edition und AVG LinkScanner. Die kostenlosen AVG-Lizenzen zum Schutz privater PCs laufen für ein Jahr. Anwender erhalten im AVG Free-Forum kostenlosen Support von anderen AVG-Nutzern.

Für den gewerblichen Gebrauch

AVG Internet Security Business Edition

Umfassender Schutz für das ganze Unternehmen

AVG Internet Security Business Edition 9.0 ist eine schnelle, intelligente Schutzlösung, die Ihre Unternehmensabläufe nicht beeinträchtigt. Das fortschrittliche Sicherheitspaket verbindet bahnbrechende Techniken wie Identitätsschutz und Cloud Security zum Schutz vor Gefahren aus dem Internet mit erweiterten Virenschutz- und Firewall-Technologien. Das ist AVGs bester proaktiver Schutz vor allen Bedrohungen. Zum Lieferumfang gehört auch die neue Rescue CD.

AVG Anti-Virus Business Edition

Unentbehrlicher Schutz für das ganze Unternehmen

Mit AVG Anti-Virus Business Edition profitieren Sie von hoch leistungsfähiger, innovativer Scantechnologie, die Ihre Unternehmensabläufe nicht beeinträchtigt. AVG LinkScanner und der erweiterte Phishing- und Firewall-Schutz sorgen für die Sicherheit Ihres Unternehmens, während Ihre Mitarbeiter online sind. Die Anwendung ist einfach zu installieren und zu verwalten. Zum Lieferumfang gehört auch die neue Rescue CD.

AVG File Server Edition

Schutz vor Viren und Spyware für File Server

AVG File Server Edition ist die richtige Lösung, wenn bereits ein Anti-Virus-Schutz für Ihre Workstations installiert ist, Sie aber noch einen Schutz für Ihren Dateiserver benötigen. Die Software enthält einen erweiterten Anti-Viren-Scanner, den AVG LinkScanner für den Schutz vor Bedrohungen aus dem Internet und eine erweiterte Phishing-Erkennung.

AVG Email Server Edition

Schutz vor Viren und Spyware für eMail-Server

Dies ist die richtige Lösung, wenn bereits ein Anti-Virus-Schutz für Ihre Workstations und Dateiserver installiert ist, Sie aber noch einen Schutz für Ihren eMail-Server benötigen. Die Software enthält einen erweiterten Anti-Viren-Scanner, den AVG LinkScanner für den Schutz vor Bedrohungen aus dem Internet, zentralisierte Spam-Abwehr und eine erweiterte Phishing-Erkennung.

AVG Server Edition for Linux/FreeBSD

Schutz vor Viren und Spam für Linux- und FreeBSD-eMail-Server

Diese Lösung ist für alle Unternehmen geeignet, die Linux/ FreeBSD-Server für eMails einsetzen. Sie bietet ausreichend Schutz vor infizierten eMails und Anhängen. AVG unterstützt alle führenden Anwendungen für Linux- und FreeBSD-eMail-Server, einschließlich PostFix, QMail, Sendmail und Exim. Das Paket enthält kostenlose Client-Software.

Über AVG Technologies

AVG ist ein weltweit führender Anbieter von Internet-Security-Lösungen und schützt 80 Millionen Endkunden und mittelständische Unternehmen in 167 Ländern vor der stetig wachsenden Zahl von Online-Bedrohungen wie Viren, Spam, Spyware und gehackten Websites. Das Unternehmen mit Hauptsitz in Amsterdam verfügt über fast zwei Jahrzehnte Erfahrung im Kampf gegen Internetkriminalität sowie eines der modernsten Labore, um weltweit Bedrohungen aus dem Web aufzuspüren, sie zu verhindern und zu bekämpfen. Das AVG Software-Modell bietet Einsteigern einen kostenlosen Antivirus-Basischutz, der online zum Download zur Verfügung steht, und erlaubt ein einfaches und preisgünstiges Upgrade auf ein höheres Sicherheits- und Schutz-Niveau sowohl in Einzel- als auch in Mehrbenutzerumgebungen. Fast 6000 Reseller, Partner und Distributoren arbeiten weltweit mit AVG zusammen, zum Beispiel Amazon.com, CNET, Cisco, Play.com, Wal-Mart und Yahoo.

Weitere Informationen zu AVG und zum vollständigen AVG Produktportfolio finden Sie auf der Homepage: <http://www.avg.de> und <http://www.avgbusiness.de>

AVG im World Wide Web

Brandaktuelle News zu aktuellen Cyberthreats im Blog von AVG Chief Research Officer Roger Thompson:

- <http://thompson.blog.avg.com/>

Allgemeine AVG-Updates:

- Treten Sie unserer Facebook-Community bei <http://www.facebook.com/avgfree>
- Folgen Sie dem AVG Twitter www.twitter.com/officialavgnews
- Registrieren Sie sich unter www.avgnews.com

Referenzen

¹ MPack:

[http://en.wikipedia.org/wiki/MPack_\(software\)](http://en.wikipedia.org/wiki/MPack_(software))

² "Storm"-Wurm:

http://en.wikipedia.org/wiki/Storm_Worm

³ Conficker:

<http://en.wikipedia.org/wiki/Conficker>

⁴ Identitäts-Diebstahl in den USA 2008: <http://uk.reuters.com/article/marketsNewsUS/idUKN0646389320090209?pageNumber=1>

⁵ Pump and Dump Schemes:

<http://www.sec.gov/answers/pumpedump.htm>

⁶ Top 10 der Sicherheits-Bedrohungen im Web 2008 (<http://www.sans.org/2008menaces/>)

⁷ 70 von 100 Top-Websites durch Malware kompromittiert

<http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=212901775>

⁸ Seriöse Webseiten als Malware-Server missbraucht

http://www.theregister.co.uk/2008/01/08/malicious_website_redirectors/

⁹ Kurzlebig und heimtückisch: Die neuen Online-Gefahren

<http://www.avg.com/press-releases-news.ndi-222533>

¹⁰ Metamorpher (selbst verändernder) Code

http://en.wikipedia.org/wiki/Metamorphic_code

¹¹ Polymorpher Code

http://en.wikipedia.org/wiki/Polymorphic_code

¹² Epidemische Ausbreitung von Malware

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=208803810>



Niederlassungen

AVG Technologies, N.V.
Claude Debussylaan 46
NL-1082 MD Amsterdam
Netherlands

AVG Technologies UK Limited
Glenholm Park, Brunel Drive
Newark, Nottinghamshire, NG24
2EG
United Kingdom

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland

AVG Technologies CZ, s.r.o.
Lidická 31
602 00 Brno
Czech Republic

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA

AVG Technologies CY Limited
Arch.Makariou III,2-4
P.C. 1505, Nicosia
Cyprus