PROTECTSTAR™

AWARD 2009

Kurztest

Emsi Software a-squared Anti-Malware 4.5

Täglich tauchen bis zu 3000 neue Schadprogramme auf die Rechner und Daten bedrohen. Für jeden neuen Schädling müssen die Hersteller neue Signaturen erstellen, damit der Schädling sicher erkannt werden kann. Das zeigt aber bereits eine Schwachstelle dieses Verfahrens auf. Bevor ein Schadprogramm überhaupt bei einem Antivirushersteller bekannt wird, muss es eine gewisse Verbreitung erfahren haben. Das bedeutet also, dass die Malwareautoren den Herstellern von Schutzprogrammen immer einen Schritt voraus sind. Um diesen Rückstand zu überwinden, versuchen die Hersteller von Schutzlösungen neue Techniken zu entwickeln, um bisher unbekannte Malware auch ohne Signatur zuverlässig erkennen zu können. Ein Ansatz ist dabei die Verhaltenserkennung, bei der das Verhalten eines jeden Programms genau beobachtet wird. Sollte ein Programm ein verdächtiges Verhalten zeigen, so wird dieses Programm gestoppt und eine mögliche Infektion verhindert. Die aus Österreich stammende Firma Emsi Software hat in ihrem Programm a-squared Anti-Malware eine solche Technologie integriert. In der aktuellen Version des Programms a-squared Anti-Malware kombiniert Emsi Software zwei Scanengines wobei mögliche Doppelerkennungen ausgefiltert werden. Der Hersteller verspricht so höchste Erkennungsleistungen bei geringer Systembelastung.

Die a-squared-Engine wurde ursprünglich für die Erkennung von Spyware und Trojanern entwickelt und hat es in diesem Bereich zu einem gewissen Bekanntheitsgrad gebracht. Die von Emsi Software selbst entwickelte Engine reagiert auch auf Cookies und Spuren von Spyware, sogenannten Traces in der Registry. Die zweite Engine, die vom ebenfalls in Österreich beheimateten Hersteller Ikarus stammt, ist ein Spezialist für das Aufspüren von Viren, Würmern und anderer Malware. Aber Emsi Software geht noch einen Schritt weiter und integriert in seine Schutzlösung eine dritte Verteidigungslinie: die Verhaltenserkennung.

Grund genug für das ProtectStar Testlab das Programm einem Praxistest zu unterziehen.

Sicherheit

A-squared verfolgt bei seinem Schutzkonzept einen etwas anderen Ansatz als bisher üblich: Während klassische Virenscanner Dateien beim Lese- oder Schreibvorgang auf schädlichen Code untersuchen (OnAccess-Scan), analysiert a-squared die Dateien erst bei der Ausführung. Dieses Verfahren nennt man auch OnExecution-Scan.

A-squared verlässt sich dabei nicht auf den klassischen Signaturscan mit einer einzelnen Scanengine, sondern prüft jede Datei bei der Ausführung gleich dreifach. Als erstes wird die Datei vor der Ausführung zunächst mit der ersten Scanengine geprüft. Dabei greift a-squared auf die Ikarus-Engine zurück. Danach erfolgt eine zweite Prüfung mit der Emsi-eigenen Scanengine. Als dritte und letzte Prüfung wird das Verhalten der Datei geprüft und beobachtet. Sollte a-squared dabei ein für Malware typisches Verhalten beobachten, so wird die Ausführung der Datei gestoppt und eine mögliche Infektion verhindert.

Diese Technik nennt Emsi selbst „Malware-IDS“, wobei IDS für „Intrusion Detecting System“ steht. Dabei kann der Anwender selber auswählen, welche verdächtigen Verhaltensweisen beobachtet werden sollen. In den Voreinstellungen untersucht das IDS jedes ausgeführte Programm auf schädliches Verhalten. Dabei wird beobachtet, ob sich das gestartete Programm wie Spyware, eine Backdoor, ein Trojaner oder Wurm, oder auch wie ein Dialer verhält. Weiterhin wird geprüft, ob der aufgerufene Prozess sich wie ein Rootkit verhält, die Host-Datei manipuliert oder versucht einen verdeckten Treiber zu installieren. Auch Prozesse, die sich in den Autostart eintragen oder andere Programme manipulieren (patchen) werden erkannt.

Der Anwender kann in den Optionen einstellen, wie a-squared mit der verdächtigen Datei umgehen soll. Da auch viele harmlose Programme für Malware typische Verhaltensweisen zeigen, gibt es die Möglichkeit, automatisch eine Regel für das Programm erstellen zu lassen. Dabei greift Emsi Software auf die Erfahrungen der a-squared Anwender zurück. Dabei wird eine Art „In the cloud“- Technologie angewendet. Jede Nutzerentscheidung bezüglich eines Programms wird da-

bei per Checksumme an Emsi Software geschickt. Für jedes Programm wird so ein Ranking erstellt. Sobald eine bestimmte Anzahl von Anwendern ein Programm als harmlos oder auch schädlich eingeschätzt haben, wird der Alarm nicht mehr gemeldet und die Regel automatisch vom Programm erstellt und angewendet. Ein Beispiel ist der erste Start des bekannten Browser Firefox. A-squared meldet ein verdächtiges Verhalten des Browser und startet eine Anfrage nach dem Userranking. Da der Firefox von mindestens 90% der Anwendern als vertrauenswürdig eingestuft wurde, erstellt a-squared automatisch eine Regel, die den Start des Firefox erlaubt. Das alles geschieht innerhalb von Sekundenbruchteilen, so dass nur ein kurzes Aufblitzen des Alarmierungsfensters zu sehen ist.

Danach erfolgt beim Aufruf des Firefox dann keine Alarm mehr. Die Prozentzahl der Anwender, die ein Programm als harmlos oder gefährlich einstufen müssen, damit eine Regel erstellt wird, lässt sich einstellen. In den Voreinstellungen liegt die Schwelle bei 90%. Es besteht die Möglichkeit diese Option vollkommen auszuschalten. Auch im Paranoid-Modus, bei dem jedes verdächtige Verhalten eines Programms gemeldet wird, hat das Userranking keine Relevanz und wird nicht berücksichtigt. Der Signaturscan greift auch nach einer Regelerstellung weiterhin. Für die regelmäßige Überprüfung des Rechners auf Malware steht der klassische OnDemand Signaturscan zur Verfügung. Hierbei kommen beide Engines zum Einsatz. Auf Wunsch werden alle Dateien einer Prüfung unterzogen, während der Wächter nur ausführbare Dateien bei der Ausführung aber nicht beim Zugriff darauf prüft.

Trotz des Einsatzes von zwei Scanengines ist die Scandauer noch befriedigend. Für einen Scan unseres Testsystems, belegt mit 178 GB und insgesamt 109886 Dateien, benötigte a-squared 44 Min. und 48 Sek. 4,47 GB saubere Dateien wurden in 3 Minuten gescannt. GData AntiVirus 2010, welches ebenfalls mit 2 Scanengines arbeitet, benötigt für die gleiche Aufgabe 4 Min. 12 Sek. Allerdings ist die Systembelastung während des Scans sehr gering, so dass ein normales Arbeiten mit den Rechner ohne Einschränkungen möglich ist. Die Erkennungsleistung des Programms ist sehr gut. Unser kleines Testset, bestehend aus 500 Samples, wurde von a-squared zu 99% erkannt. Zum Vergleich wurde das gleiche Testset von vier weiteren aktuellen Virenscannern untersucht. Alle Produkte führten den Scan mit Signaturstand vom 03.09.09 aus. Lediglich der Scanner von GData, welcher ebenfalls mit zwei Scanengines arbeitet, erreichte eine geringfügig höhere Erkennungsrate.

Scanergebnisse ausgewählter Virenscanner

A-squared 4.5	Avira 9.0	BitDefender 2010	GData 2010	Kaspersky 2010
99,0%	97,6%	97,8%	99,4%	95,2%

Dieser gute Eindruck wird durch die Beobachtungen, die wir während der Testreihen auf der Seite www.virustotal.com gemacht haben, bestätigt. Auch hier zeigt a-squared sehr gute Erkennungsleistungen. Natürlich darf dabei die Anzahl der Fehlalarme nicht außer Acht gelassen werden. Allerdings nimmt man bei Emsi Software dieses Problem ernst und korrigiert Fehlalarme umgehend nach Bekanntwerden. Zu Beginn der Testreihen wurde beispielsweise in dem Opensource Browser Iron die Malware Trojan.Banload.a entdeckt. Nach zwei Tagen wurde der Fehlalarm – ohne dass er von uns gemeldet wurde - korrigiert.

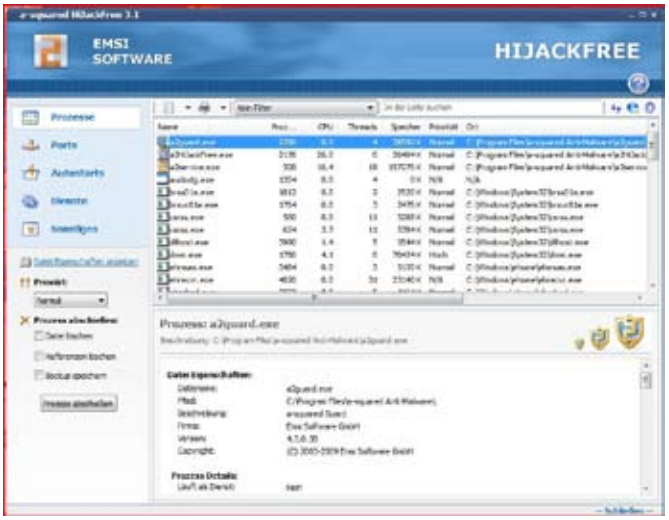
Ein Http-Scanner ist ebenso wie ein Mailscanner nicht vorhanden. a-squared schlägt beim Surf-Schutz einen anderen Weg ein, in dem es nicht den gesamten Inhalt einer Website scannt, sondern vielmehr vorher eingreift, in dem es den Zugriff auf gefährliche Hosts bzw. Webserver von vornherein verbietet. In den Voreinstellungen warnt a-squared vor diesen Hosts und erwartet eine Benutzerinteraktion, wobei die die Option “blockieren” vorgewählt ist. Für jede getroffene Entscheidung wird eine Regel angelegt, so dass bald ein individuelles Regelwerk angelegt ist und der Anwender unbehelligt Surfen kann. Das Programm greift also ein, bevor überhaupt Schadcode auf den Rechner gelangen kann. Erstaunlich ist dabei die Trefferquote die Emsi Software mit diesem Verfahren erreicht. Ebenso erstaunlich ist, auf welch große Anzahl unseriöse Hosts man bei einer einfachen Suche nach einem Wallpaper stößt. Mitunter ist a-squared an dieser Stelle etwas übereifrig. So wird der Aufruf der Seite freemail.web.de unterbunden, da auf dieser Seite das Programm „Smartsufer“ erhältlich ist. Bei diesem Programm handelt es sich um eine Einwahlsoftware die von web.de zur Verfügung gestellt wird. A-squared vermutet hinter diesem Programm – vollkommen zu Recht – einen Dialer und unterbindet den Zugriff auf die Seite.

Der fehlende Mailscanner ist kein wirkliches Risiko, da weiterhin jede ausführbare Datei dreifach geprüft wird. Was mit diesem Verfahren nicht unterbunden werden kann ist, dass Malware per Mail auf den Rechner gelangt oder auch per Mail weitergegeben wird. Hier greift a-squared konzeptbedingt nicht ein.

Benutzerfreundlichkeit

Nach der problemlosen Installation des Programms, welche ohne Neustart auskommt, begrüßt den Anwender zunächst ein Einrichtungsassistent, der durch die ersten Schritte führt. Dabei wird zunächst ein Update angestoßen und ein erster Systemscan ausgeführt, bevor der Echtzeitscanner seine Arbeit aufnimmt.

Leider gibt es keine Restzeitanzeige für die Scandauer oder eine Möglichkeit den Rechner nach einem Scan automatisch herunterzufahren. Auch eine Berichtshistorie gibt es nicht;



die sehr aussagekräftigen und dabei übersichtliche Berichte können nur direkt nach dem Scan manuell abgespeichert werden. Weiterhin würden wir uns weitergehende Konfigurationsmöglichkeiten für den OnDemand-Scan wünschen. Die Grundeinstellungen des Programms sind praxisgerecht ausgewählt und bieten einen guten Kompromiss zwischen Sicherheit und Komfort. Grundsätzlich werden bei einer Benutzerinteraktion Regeln angelegt, so dass jedes Programm nur einmal zu einer Abfrage führt. Dabei ist als empfohlene Aktion immer „blockieren“ voreingestellt, so dass ein unbedachter Klick nicht zu einer Malwareinfektion führt.

Die Meldungen, die vom Echtzeitscanner ausgegeben werden sind verständlich und dürften den Anwender generell nicht vor Probleme stellen, zumal die vorgeschlagenen Aktionen sehr sinnvoll gewählt sind und großer Wert auf Sicherheit gelegt wird. Es bedarf einiger Anstrengungen, um eine von a-squared Anti-Malware als bedrohlich eingestufte Datei zu starten. Weiterhin ist die oben beschriebene community basierende Alarmreduktion eingestellt, so dass ein für einen Großteil der bekannten Programme automatisch Regeln erstellt werden.

In den Standardeinstellungen sucht das Programm stündlich nach neuen Signaturen. Dieses Intervall kann beliebig angepasst werden. Neue Signaturen werden durch ein dezentes Popup über dem Infobereich und durch ein kleines Fenster beim Überfahren des Trayicons mit der Maus angezeigt.

Diese Lösung finden wir sehr übersichtlich, da so der aktuelle Singnaturstand erfragt werden kann, ohne die Oberfläche des Programms öffnen zu müssen. Laut Hersteller sucht a-squared drei Minuten nach dem Systemstart nach neu verfügbaren Signaturen. Während der Testreihen wurden erst nach ca. 10 Minuten neue Signaturen heruntergeladen. Dieser Zeitraum erscheint uns zu lang.

Unsere Testreihen haben gezeigt, dass Emsi Software in der Regel 4-5 mal am Tag neue Signaturen bereitgestellt.

Performance

Dass der Echtzeitwächter nur bei der Ausführung einer Datei in Aktion tritt macht sich in der hervorragenden Performance bemerkbar. Es ist erstaunlich, welche Performance auch in älteren Systemen stecken kann, wenn man bereit ist auf einen OnAccess-Scan, wie ihn übliche Virenschutzprogramme einsetzen, zu verzichten.

Das Durchsuchen großer Ordner oder Multimediasammlungen wird in keiner Weise verzögert, da der Echtzeitscanner erst in dem Moment greift, in dem eine Datei ausgeführt wird. Lediglich beim Starten von Programmen ist eine leichte Verzögerung bemerkbar. Das Kopieren oder Packen und Entpacken von Dateien wird durch die besondere Arbeitsweise des Programms in keiner Weise beeinflusst. Allerdings genehmigt sich a-squared rund 180 MB Arbeitsspeicher, da die kompletten Scanengines inklusive Signaturen im Arbeitsspeicher gehalten werden. Ein großzügig bemessener Arbeitsspeicher ist also absolut empfehlenswert. Der Surfschutz beeinflusst die Surfperformance nicht. Der Systemstart wurde durch den Einsatz des Programms nicht spürbar beeinträchtigt.

Ausstattung

Als weitere Zugabe ist in dem Programm noch die Komponente Hijack-Free enthalten, die einen umfassenden Überblick über die auf dem Rechner installierten Programme und Prozesse bietet. Eine komfortable Verwaltung der beim Systemstart geladen Komponenten und Dienste ist ebenfalls vorhanden und geht weit über die von Windows bereitgestellten Möglichkeiten hinaus. Diese Komponente ist in der Hand eines erfahrenen Anwenders ein mächtiges Werkzeug.

Vom Ausstattungsumfang kann a-squared nicht mit einer ausgewachsenen Security-Suite mithalten. Komponenten wie Firewall oder Spamfilter fehlen.

Hier muss also auf die in jedem Windowssystem enthalten Komponenten- wie die Windows-Firewall oder den im Mailclienten enthaltenen Spamfilter- zurückgegriffen werden.

Potenziell unsicherer wird ein Windowssystem dadurch keinesfalls; vielmehr werden mögliche Systemkonflikte vermieden und die Systemressourcen geschont. Was somit wieder ein Vorteil gegenüber dem Einsatz einer Security Suite wäre.

Support

Sollten Fragen zum Programm auftreten, so hilft die verständliche und ausführliche Onlinehilfe weiter. Auch ein sehr gut moderiertes Forum, welches direkt aus dem Programm heraus aufgerufen werden kann, steht zur Verfügung.

Das Forum wird direkt von den Entwicklern betreut, so dass hier schnell und kompetent geholfen wird. Auf der Herstellerseite sind ausführliche FAQs verfügbar. Auch Hinweise zur Computersicherheit im Allgemeinen sind verfügbar. Interessierte Anwender finden weiterführende Dokumentation über die a-squared Technologie. Alle Dokumente sind dabei sehr ausführlich und verständlich geschrieben.

Fazit

A-squared Anti Malware 4.5 von EMSI Software hinterließ in den Testreihen durchweg einen sehr positiven Eindruck.

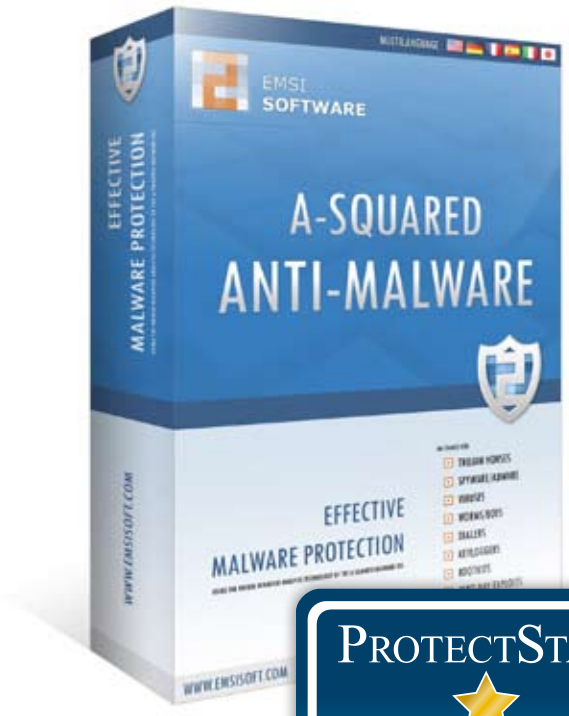
Die Erkennungsleistung ist sehr gut und durch die zusätzliche Verhaltensüberwachung wird ein sehr hohes Schutzniveau erreicht. Die zunächst auftretenden Nachfragen des Programms reduzierten sich mit fortlaufender Nutzung sehr rasch, so dass immer weniger Interaktion notwendig wurde. Die Oberfläche ist klar strukturiert und übersichtlich.

Die Software zeigte kaum negativen Einfluss auf die Systemperformance und lief absolut stabil. A-squared richtet sich an Anwender die ein hohes Schutzniveau mit äußerst geringen Performanceeinbußen wünschen und dafür bereit sind, auf einen Http- oder Mailscan zu verzichten. Gerade der Umstand, dass die Dateien erst bei der Ausführung per Signaturscan geprüft werden, sowie die Verhaltensüberwachung, machen den entscheidenden Unterschied aus.

Das Programm ist auf der Website unter www.emsisoft.com zum Preis von 30€ als Download erhältlich. Weiterhin ist eine Freewareversion erhältlich, bei der jedoch der Echtzeitschutz und das Modul Hijack-Free fehlt.

Aufgrund der hervorragenden Gesamtleistung wird a-squared Anti-Malware 4.5 der ProtectStar Award 2009 verliehen.

Oliver Rosenow
o.rosenow@protectstar.com



Anregungen, Kritik und Spenden

Das ProtectStar™ Test Lab arbeitet strikt unabhängig.

Die hier durchgeführten Testanalysen, die Aufbereitung und Ausarbeitung der Testresultate, Design des Testberichts, Übersetzungen, Publizierungen, Arbeitszeiten, Löhne, Bereitstellungen, uvm. wurden ausschließlich von der ProtectStar™, Inc. finanziert. Die im Testbericht genannten Hersteller stellten lediglich und nur zum Teil die für die Testreihen benötigten Testversionen bzw. Lizenzen bereit.

Um die Testreihen in Zukunft weiter verbessern zu können, dankt ProtectStar™ jeder Art von Anregung und Kritik seiner Leserinnen und Leser. Bitte teilen Sie uns mit, was Ihnen besonders gut gefallen hat und welcher Test für Sie hätte ausführlicher behandelt werden können.

Sofern Ihnen der Testbericht gefallen und Ihnen bei einer möglichen Kaufentscheidung geholfen hat oder Sie durch ergänzendes Expertenwissen im Bereich der IT-Sicherheit Neues erfahren konnten, so danken wir Ihnen für **Ihre materielle Unterstützung** der wohltätigen **ProtectStar™ Foundation**

(www.protectstar-foundation.org)

Ihre Unterstützung kommt weltweit **gemeinnützigen Hilfsprojekten** zugute. Speziell in den Bereichen Bildung, Gesundheit und IT für Schüler wird Ihre Hilfe sehr gerne angenommen.

Kontakt

Corporate Headquarter:
ProtectStar, Inc.
TestLab
444 Brickell Avenue
Suite 51103
33131 Miami, FL
USA

Phone: +1 888 218 4123
Fax : +1 888 218 8505
e-Mail: testcenter@protectstar.com
Web : www.protectstar-testlab.org

European Headquarter:
ProtectStar, Inc.
Test Lab
Daws House
33-35 Daws Lane
London NW7 4SD
UK

Phone: +44 20 8906 6651
Fax : +44 20 8906 6611
e-Mail: testcenter@protectstar.com
Web : www.protectstar-testlab.org

Copyright