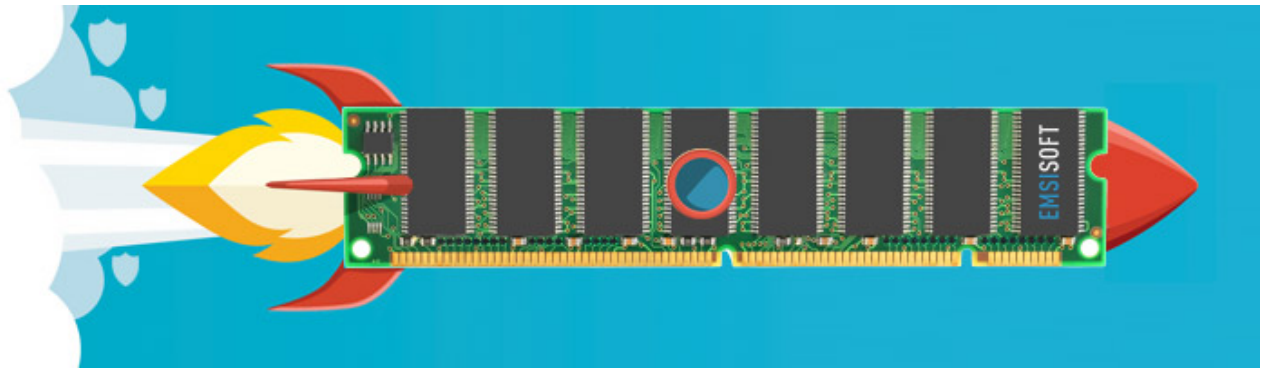
Darum brauchen Antiviren-Programme viel RAM

Darum verbrauchen Antiviren-Programme so viel RAM – und das ist auch gut so!

Mit freundicher Genehmigung von EMSISOFT
In Sicherheitswissen by Jochen on April 13, 2016 | Français, English, Deutsch
In vielen Computer-Blogs und -Magazinen bekommen Sie Tipps dazu, wie Ihr Computer schneller arbeiten soll, indem Sie die Auslastung der Hardwareressourcen verringern. Ein paar Gigabyte freier Speicherplatz auf der Festplatz sind sicher durchaus von Vorteil; für das schnelle Kurzzeitgedächtnis Ihres Computers, den Arbeitsspeicher (RAM. Random Access Memory) gilt dies jedoch nicht unbedingt.

Der RAM ist die schnellste Komponente Ihres PCs



Hier zunächst einmal ein paar Zahlen: Eine konventionelle Festplatte (HDD) bietet in der Regel Übertragungsraten von etwa 80-160 MB/Sekunde. Moderne Solid-State-Disks (SDD), bei denen Speicherchips ähnlich denen von SD-Karte, wie sie sich in Kamera oder Ihrem Smartphone finden, zum Einsatz kommen, bieten Übertragungsraten von etwa 200-400 MB/Sekunde. Der RAM Ihres Computers, dessen Inhalt ohne Stromzufuhr verloren geht, bietet hingegen Übertragungsraten von 10-20 GB/Sekunde. Das ist 100 Mal schneller als jede

Festplatte!

Wo würden Sie also als Programmierer eher Ihre Programme ausführen? Wohl offensichtlich im RAM.

So verwaltet Windows den RAM

Beim Start von Windows werden alle Programme, die Bestandteil des Systems sind, von der Festplatte gelesen und in den RAM geladen. Von dort aus kann der Prozessor darauf effizient zugreifen. Die Arbeitsdaten, die von den Programmen erstellt werden, werden zusammen mit anderen Programmen im RAM vorgehalten. Das bedeutet also: je mehr Programme Sie öffnen und mehr Daten geladen werden, desto eher geht Ihnen der Arbeitsspeicher aus.

Heutzutage liegt die Größe des Arbeitsspeichers üblicherweise zwischen 2 und 16 GB, doch es kann vorkommen, dass Windows mehr RAM benötigt, als physisch vorhanden ist. Dies ist kein Grund zur Sorge, da sich die Entwickler bei Microsoft dieser Gefahr bewusst waren und daher die sog. Auslagerungsdatei vorgesehen haben. Deren Funktionsprinzip ist einfach: Programme oder Daten, die nicht häufig verwendet werden, werden in eine "virtuelle Arbeitsspeicherdatei" auf der Festplatte geschrieben (diese ist versteckt als "c:\pagefile.sys"). So erhalten Sie zusätzlichen freien RAM. Allerdings müssen alle Daten aus dem virtuellen RAM von der langsamen Festplatte gelesen werden, bevor sie wieder verwendet werden können.

Dadurch wird Ihr Computer zunehmend langsamer; und Sie fragen sich wohl, was mit Ihrem Computer los ist. Seien Sie jedoch unbesorgt, es wurden lediglich Daten in die Auslagerungsdatei ausgelagert.

Gute oder schlechte hohe Speicherauslastung?

Soviel haben wir also bisher gelernt: Der Arbeitsspeicher ist schnell, nutzen wir ihn also! Eine Senkung des Speicherverbrauchs von beispielsweise 70 auf 40 % bringt nicht viele Vorteile mit sich, denn freier RAM sind verschenkte Ressourcen. Weder senkt es den Stromverbrauch noch bringt es jegliche Leistungsvorteile mit sich. So gesehen sollten Sie so viel Arbeitsspeicher wie möglich für bestmögliche Systemleisung nutzen.

Ab einem gewissen Punkt ist er jedoch ausgeschöpft, und Windows wechselt auf

die Auslagerungsdatei. Sie können verhindern, dass Windows dies allzu oft tut, indem Sie ausreichend RAM einbauen. Arbeitsspeicher ist günstig zu erwerben, und eine größerer RAM-Baustein ist oftmals der einfachte Weg, um die Lebenszeit Ihres alten Computers um ein oder zwei Jahre zu verlängern. Ich persönlich bin zum Beispiel ein anspruchsvoller Nutzer, benötige aber selten mehr als 4 GB RAM.

Warum verbraucht Antiviren-/Anti-Malware-Software überhaupt so viel RAM?

Oftmals kommen uns Kundenbeschwerden über hohen RAM-Verbrauch zu Ohren. Nun, unser Ziel ist es, Malware zu erkennen. Dazu benötigen wir Erkennungs-/Suchmuster, um Dateien mit den Bedrohungen in unserer Datenbank zu vergleichen. Diese Muster (die manchmal auch als Fingerabdrücke oder Signaturen bezeichnet werden) sind nicht wirklich groß, aber da im Internet Unmengen von Bedrohungen kursieren, ist die Zahl der benötigten Signaturen beträchtlich.

Derzeit kommen bei unserer Software mehr als 7 Millionen Malware-Signaturen zum Einsatz. Um all diese in den RAM zu laden, sind etwas mehr als 200 MB notwendig. Das hört sich viel an, aber bedenken Sie: dies entspricht im Durchschnitt einer kurzen Sequenz von 28 Byte, mit der bestimmt werden kann, ob eine Datei gefährlich ist oder nicht. Das können Sie sich folgendermaßen vorstellen: Denken Sie an eine Textsequenz mit gerade einmal 28 Zeichen, die es in einer Bibliothek mit 1 Milliarde Büchern zu finden gilt, ohne dass Sie sich einen einzigen Fehler erlauben dürften. So hat ein Malware-Scanner 7 Millionen Signaturen gegen etwa 300.000 Dateien auf Ihrer Festplatte zu prüfen – und das in Sekundenbruchteilen!

Von einem technischen Standpunkt aus ist es unmöglich, einfach so auf 7 Millionen Signaturen zu verzichten. Diese müssen für eine gute Erkennung an einem Ort gespeichert werden (und nicht für minimale Erkennung wie zum Beispiel in Windows Defender). Des Weiteren muss ein schneller Zugriff darauf möglich sein, damit jede neue und geänderte Datei geprüft werden kann, die ihren Weg auf Ihren Computer findet. Und noch dazu so schnell, dass Sie nicht einmal merken, dass im Hintergrund greprüft wird. Hier kommt der Arbeitsspeicher ins Spiel.

Mit dieser Herausforderung sehen wir uns nicht nur bei Emsisoft konfrontiert, dies gilt ebenso für unsere Konkurrenten. Sämtliche signaturbasierten Antiviren- oder Anti-Malware-Programme benötigen einiges an Arbeitsspeicher, um Ihren Computer effizient zu schützen.

Ein gut gehütetes Geheimnis: Antiviren-Programme schweigen sich gern über ihren RAM-Verbrauch aus

Hoher RAM-Verbrauch verkauft sich nicht gut, aber was soll man tun, wenn er unumgänglich ist? Er wird einfach versteckt. Dazu gibt es zwei häufig genutzte Techniken, durch die ein umfangreiches Programm kleiner aussieht.

1. **Verwendung der Auslagerungsdatei:** Wie vorher beschrieben verschiebt Windows weniger häufig genutzte Programmteile auf die langsame Festplatte. Programme können diesen Vorgang ebenfalls erzwingen und sich von Windows in regelmäßigen Abständen in die Auslagerungsdatei verschieben lassen. Der Windows Task-Manager zeigt dann sehr geringe Arbeitsspeichernutzung an; allerdings müssen Sie dann beim Zugriff auf das Programm etwa 1-3 Sekunden Verzögerung in Kauf nehmen. Diese Zeit wird nämlich zum Auslesen von der Festplatte benötigt.

Name	4% CPU	35% Memory	0% Disk	0% Network
Emsisoft Protection Service	0%	2,8 MB	0,1 MB/s	0 Mbps
Emsisoft Real-Time Protection	0%	2,0 MB	0 MB/s	0 Mbps
Emsisoft Security Center	0%	4,6 MB	0 MB/s	0 Mbps

Geringerer Speicherverbrauch

In Emsisoft Anti-Malware und Emsisoft Internet Security haben Sie vollständige Kontrolle über diese Funktion. Schalten Sie “Speicherverbrauch-Optimierung aktivieren” in den allgemeinen Einstellungen ein, damit die Software niemals in die Auslagerungsdatei verschoben wird. Dies erhöht im Allgemeinen die Systemleistung, sofern genügend RAM vorhanden ist.

2. **Verwendung von Systemtreibern:** Der Windows Task-Manager zeigt nur laufende Programme und Dienste an, jedoch keine Treiber. Treiber sind Kernelmodule, die direkt vom System für bestimmte grundlegende Funktionen geladen werden. Einige Anbieter von Antiviren-Software laden in ihren Treibern Hunderte Megabyte an Daten, um Ihnen geringen Speicherverbrauch vorzutäuschen. Dies können Sie erkennen, wenn Sie den von allen laufenden Programmen verwendeten Speicher zusammenzählen und dann mit dem Wert des insgesamt genutzten RAM vergleichen. Sollte der Unterschied beträchtlich ausfallen, wird Ihnen wohl hoher Speicherverbrauch verschwiegen.

Wenn jedes Jahr sich die Menge an Bedrohungen verdoppelt, müsste doch eigentlich der Speicherverbrauch in gleichem Maße zunehmen?

Das Gute an Malware ist, dass viele Varianten in der freien Wildbahn einander ähneln. Die Zahl von Malware-Familien ist begrenzt, und oft unterscheiden sich Varianten lediglich um wenige Bytes. Daher können wir eine größere Anzahl an Bedrohungen mit weniger, aber dafür intelligenteren Signaturen erkennen. Dadurch wächst die Zahl der zur bestmöglichen Erkennung notwendigen Signaturen nicht annähernd so schnell wie die Zahl der Bedrohungen im Internet.

Fazit: Nutzen Sie Ihren RAM

Öffnen Sie einmal den Task-Manager (mit Rechtsklick auf die Taskleiste, dann wählen Sie “Task-Manager starten”) und prüfen Sie, wie viel RAM effektiv bei starker PC-Nutzung vewendet wird. Sofern sich die Nutzung nicht nahe der physischen Grenze ansiedelt, können Sie die Funktion “Speicherverbrauch-

Optimierung aktivieren” in Emsisoft ausschalten, um die bestmögliche Leistung zu erzielen.

Einstellungen der Emsisoft-Schutzsoftware

Wählen Sie Ihre Antiviren-/Anti-Malware-Lösung nicht nur anhand von Rezensionen über den Speicherverbrauch, sofern Sie über ausreichend RAM verfügen (mindestens 2 GB).