Schutz für Ihre Dateien, aber auf Kosten Ihrer Privatsphäre?

Antivirensoftware: Schutz für Ihre Dateien, aber auf Kosten Ihrer Privatsphäre?

In Emsisoft Lab, Emsisoft News, Sicherheitswissen by Jochen on June 26, 2015 | Français, English, Deutsch

> ***Unter "Datenschutz" versteht man die Fähigkeit einer Person oder einer Gruppe, sich selbst oder Informationen über sich selbst abzuschirmen und sich so selektiv auszudrücken.****[Wikipedia]*

Wir möchten etwas klarstellen: Datenschutz ist essenziell. Punkt.

Heutzutage scheinen uns große Unternehmen und Regierungen hier jedoch tendenziell zu widersprechen. Sie möchten uns glauben machen, dass Sicherheit und Bequemlichkeit immer auf Kosten unserer Privatsphäre gehen. Wir sind allerdings anderer Meinung. Das Missbrauchsrisiko von massenhaft gesammelten Daten sticht in unseren Augen jedes Argument gegen vermeintlich notwendige Funktionalität, die auf Analyse dieser Datenmengen basiert.

Nur wenige Menschen sind sich dessen bewusst, dass die größte Gefahrenquelle für Ihre Privatsphäre tatsächlich eine Software ist, die sie selbst auf ihrem Rechner installiert haben und generell auf den meisten Rechnern läuft. Eine Software, die sie in dem Glauben erworben haben, sie schütze ihre Daten: Antivirensoftware.

Funktionen im Virenschutz, die auf Kosten Ihrer Privatsphäre gehen

Es gibt ein paar höchst fragwürdige Funktionen in gebräuchlicher Schutzsoftware, die wir ein bisschen genauer unter die Lupe nehmen möchten:

1) Prüfen und Blockieren gefährlicher URLs

Fast alle Internetsicherheitslösungen behaupten, Sie vom Zugriff auf gefährliche und betrügerische Websites abzuhalten und so gegen Malware-Downloads und Betrugsversuche zu schützen. Dazu werden üblicherweise alle Website-Adressen, die Sie besuchen, an einen zentralen Server weitergeleitet, der die Domainnamen und Pfade gegen eine riesige Datenbank mit gefährlichen URLs prüft.

Sie fragen sich wohl, warum diese Scans nicht lokal auf Ihrem Computer durchgeführt werden können. Der Grund hierfür erfordert ein wenig technisches Verständnis, ist aber nicht weiter kompliziert: Für eine lokale Überprüfung von Adressen wäre es notwendig, die gesamte Datenbank über Online-Updates in regelmäßigen Abständen auf Ihren Computer zu übertragen und aktuell zu halten. Das Problem dabei ist folgendes: es gibt tatsächlich Millionen bekannter bösartiger Websites, die sich häufig ändern. Online-Updates für Schutzsoftware würden für die meisten Nutzer tagtäglich eine deutliche Mehrbelastung bedeuten, da Hunderte Megabyte an Daten auf den neuesten Stand gebracht werden müssten. Das möchte Ihnen niemand zumuten. Daher ist es viel effizienter, jede besuchte Adresse an einen Server zu senden, der die ganze Arbeit übernimmt und einfach eine Meldung (“sicher” oder “gefährlich”) zurückgibt.

Der Nachteil daran? **Antivirensoftwareanbieter könnten ALLE Ihre besuchten Websites nachverfolgen**. Und es kommt noch schlimmer: Einige Anbieter können sogar verschlüsselte Daten auslesen, die Sie auf Online-Banking-Portalen oder anderen vermeintlich privaten Kommnikationskanälen eingeben. Diese riesigen Datenbankserver sind natürlich bestmöglich geschützt. Seien Sie sicher, dass Daten niemals 100 % sicher sind. Denken Sie einmal kurz darüber nach, was geschähe, falls ein Softwarehersteller aus irgendeinem Grunde die Kontrolle über seine Server verlieren würde und Ihre Surfgewohnheiten mitsamt privater Daten von Kriminellen genutzt werden könnten.

2) Cloud-basierte Dateiprüfung

Vor ein paar Jahren galt jedes Softwareunternehmen, das sich nicht am “Cloud”-Hype beteiligte, als unrentabel und altbacken. Es besteht kein Zweifel daran, dass Cloud-Computing – also die Verlagerung ressourcenlastiger Berechnungen von lokalen Rechnern auf Server – sich als effizienter Schritt erwiesen hat. Seit Veröffentlichung der ersten Antivirenprogramme werden Dateien lokal auf dem Rechner geprüft. Antivirensoftwareanbieter erstellen eine Datenbank mit Fingerabdrücken/Signaturen von Viren und anderen Bedrohungen, senden diese Sammlung eindeutiger Kennzeichen an die Antivirensoftware auf Ihrem Computer, wo dann alle lokalen Dateien mit jeder dieser Signaturen verglichen werden.

Beim Cloud-Scannen wird dieser Vorgang sozusagen umgekehrt. Es werden Signaturen aller potenziell verdächtigen Dateien auf Ihrem lokalen Rechner erstellt und anschließend auf Cloud-Server hochgeladen, auf denen diese dann gegen eine große Datenbank mit bekannten Bedrohungen geprüft werden. Signaturen sind üblicherweise kurze Folgen aus Buchstaben und Ziffern, sodass kein Antivirensoftwareanbieter jegliche Dateiinhalte wiederherstellen kann. Jedoch können sie erkennen, welche Programme auf Ihrem PC laufen, falls das gleiche Muster bereits vorher zu finden war, und andere Metadaten mit dem Datensatz verknüpft wurden.

Viele Anbieter gehen sogar noch einen Schritt weiter: Sie laden nicht einen einzigartigen Dateimarker auf die Server, sondern die gesamte Datei, die dann dort untersucht werden kann. Bei Programmdateien besteht hier normalerweise kein Risiko. Aber seien wir ehrlich, hat jemals ein Antivirensoftwareanbieter seine Kriterien bei der Wahl von Dateien offengelegt, die hochgeladen werden? Sie müssen blind darauf vertrauen, dass keinerlei Ihrer privaten Datendateien mitgeschickt werden.

3) Sammeln von Metadaten

Manchmal kann man mit Metadaten eines Computer mehr anstellen, als mit gesammelten Datendateien. Mit Metadaten werden allerlei Arten von Informationen wie dem Computernamen, dem Benutzernamen, der IP-Adresse, dem Land, dem Betriebssystem, ausgeführten Programmen, deren Versionsnummern, Hardwarekomponenten oder dergleichen bereitgehalten. Durch Sammeln und Verknüpfen dieser Daten lässt sich ein recht genaues Bild jedes Computers zeichnen und in gewissem Maße die Anfälligkeit für Online-Bedrohungen ausmachen.

Aus diesen Daten lässt sich natürlich auch viel über die Person herauslesen, die vor dem PC sitzt. Durch Verknüpfen der Daten lässt sich erkennen, welche Software wie lange genutzt wurde, wo Sie leben, wo Ihre Interessen liegen, welcher Altersklasse Sie angehören, für welche Hardware Sie Geld ausgeben usw.

AV-Comparatives, eine angesehene Organisation, die sich Tests von Sicherheitssoftware widmet, führte 2014 eine Untersuchung der Datenübertragung bei Internet-Sicherheitsprodukten durch. Hier ein kurzer Überblick der Ergebnisse:

- 8 von 21 Antivirenprogrammen übermitteln Hardwareinformationen, 5 legen diese Informationen gar nicht offen.
- 6 von 21 Antivirenprogrammen übermitteln Informationen über laufende Programme; 4 machen dazu keine Angaben.
- 18 von 21 übermitteln Adressen von Websites (sowohl gut- als auch bösartige).
- 5 von 21 übermitteln “verdächtige” nicht ausführbare Dateien (wie Dokumente); 7 machen dazu keine Angaben.
- 6 von 21 geben den Nutzern nicht einmal die Möglichkeit, sich dagegen auszusprechen.

AV-Comparatives empfiehlt, die Datenschutzbestimmungen und Endnutzervereinbarungen der Anbieter genau zu lesen, sodass Nutzer eine fundierte Entscheidung treffen können. So heißt es: “Nutzer sollten sich nicht zur Verwendung kostenloser Produkte verleiten lassen, bei denen obligatorisch persönliche Daten übermittelt werden (Datamining, die Auswertung größerer

Datenmengen, ist ebenfalls ein Geschäftsmodell wie die Integration von Drittanbieter-Toolbars, die eigens Informationen sammeln).”

Antivirensoftwareanbieter, die mit Nutzerdaten handeln

Nutzer, die auf Sicherheitssoftware von Avast setzen, sollten sich im Klaren darüber sein, dass ihre Surfgewohnheiten von einem Unternehmen namens Jumpshot überwacht werden. Wie Avast kürzlich bekanntgab, erstellt Jumpshot Statistiken auf Grundlage der besuchten Websites. Hierbei könnte es sich um beeindruckende, wirklich interessante Statistiken handeln. Bedenken Sie allerdings, dass Sie selbst herzlich wenig Kontrolle darüber haben, was mit all diesen Daten geschieht, sobald sie einmal an Länder mit anderen rechtlichen Bestimmungen gesendet werden. Das Installationsprogramm von Avast behält sich ebenso das Recht vor, Nutzungsdaten zu übermitteln (ohne zu erläutern, was dies genau bedeutet).

Schutzalternativen, die Ihre Privatsphäre nicht beeinträchtigen

Die gute Nachricht für alle jene unter Ihnen, die fürchten es gäbe keine Alternativen gegen Malware ohne Datensammlung: Es gibt sie durchaus. Natürlich ist der Aufwand bei der Programmierung etwas höher sein (was dem Softwareanbieter mehr Arbeit macht), aber dennoch arbeiten diese Alternativen mindestens genauso effizient wie jene Lösungen, die Ihre Privatsphäre beeinträchtigen.

Blockieren von Website-Domains statt Website-Adressen

Anstatt einzelne Website-Adressen zu blockieren, setzen wir bei Emsisoft Anti-

Malware und Emsisoft Internet Security auf eine lokal gespeicherte schwarze Liste mit bösartigen Domainnamen. Der Großteil der Malware wird heutzutage über kompromittierte Webserver verbreitet. Sollte ein bestimmter Server kompromittiert werden, so vertrauen wir so lange keiner Website auf diesem Server mehr, bis dieser wieder sauber ist. Wir blockieren den Zugriff auf den gesamten Server, wodurch weniger Daten in der schwarzen Liste gespeichert werden müssen. Damit kann Cloud-basiertes Scannen vermieden und die Prüfung lediglich lokal auf Ihrem Computer durchgeführt werden. Updates dieser Datei werden alle 15 Minuten ausgeliefert. Tests haben bestätigt, dass dieser Ansatz oftmals sogar Cloud-basierten Scans überlegen ist.

Vermeidung von Dateiuploads beim Cloud-Scannen

Bei Produkten von Emsisoft werden nie ohne Ihre vorherige Zustimmung Dateien auf unsere Server hochgeladen. Die benötigten Datenmengen bei Scans, halten wir minimal. In den meisten Fällen ist nur ein MD5-Hash (eine Prüfsumme mit 32 Zeichen) notwendig, um die Sicherheit eines Programms zu überprüfen. Nutzerdokumente werden niemals hochgeladen.

Minimiale Metadatensammlung

AV-Comparatives bestätigt in seinem Bericht, dass Emsisoft einer der Antivirensoftwareanbieter auf dem Markt, die sich am meisten um Datenschutz bemühen. Bei unseren Produkten werden möglichst wenige Informationen übermittelt, mit Hilfe derer sich womöglich detaillierte Nutzerprofile erstellen ließen.

Datenschutzoptionen für unsere Nutzer

Mit der kürzlich veröffentlichten Version 10 unserer Sicherheitsproduktreihe sind wir unseren Mitbewerbern in punkto Datenschutz wieder einmal einen Schritt voraus. Alle Einstellungen, welche Auswirkungen auf Ihre Privatsphäre haben können, finden Sie in einem neuen Abschnitt namens “Datenschutzeinstellungen”. Dort können Sie darüber entscheiden, ob Statistiken auf Grundlage der erkannten Malware erstellt werden. Ebenso entscheiden Sie weiterhin über Ihre Teilnahme am Emsisoft Anti-Malware Network, mit Hilfe dessen die Erkennung von Malware

für alle Nutzer verbessert wird. Optionen zur Deaktivierung der SSL-Verschlüsselung sämtlicher Serverkommunikation und die Erstellung von Absturzberichten finden sich auch dort.

Bei der Installation unserer Software können Sie entscheiden, ob Sie mit dem Teilen Ihrer Daten einverstanden sind oder nicht. Wir zwingen Sie niemals zur Teilnahme, noch geben wir Standardeinstellungen dieser Optionen vor – allein Sie entscheiden.

Fazit: Datenschutz ist kein Schnee von gestern

Emsisoft ist der lebende Beweis dafür, dass Sicherheit nicht auf Kosten des Datenschutzes gehen muss. Ganz im Gegenteil, es lässt sich der gleiche, wenn nicht sogar besserer Schutz verwirklichen, ohne Ihre Privatsphäre in Mitleidenschaft zu ziehen.

Wir wünschen eine schöne Zeit im Sinne Ihrer Privatsphäre!