Foto: skyla80 Shutterstock.com

Wölfe im Schafspelz

Die Anbieter von Gratis-Virenscannern sammeln Nutzerdaten nicht nur, sondern verkaufen sie auch. Der Unterschied zu jenen, vor denen sie Schutz bieten sollen, schwindet dahin.

Computer, Tablets und Smartphones dienen vielen von uns schon längst als eine Art erweitertes Gehirn. Umso wichtiger ist es, unsere darauf gespeicherten Daten vor unbefugtem Zugriff zu schützen. Ein stets aktuell gehaltener Virenscanner ist dabei das Mindeste, womit man sich Basissicherheit verschafft. Doch was, wenn gerade diese Software, die eigentlich Malware aufspüren sollte, Informationen über uns weitergibt?

Das Ziel: Geld verdienen

Genau das geschieht – und nicht nur bei AVG, jenem Unternehmen, das zuletzt für Schlagzeilen sorgte, weil es immerhin so ehrlich war, die Absicht des Datenverkaufs offen zuzugeben. Das Unternehmen, das neben Avast und Avira zu den größten Anbietern von kostenloser Antivirensoftware zählt, hat mit Mitte Oktober 2015 seine Datenschutzbestimmungen geändert. Im neuen Vertragstext räumt sich AVG das Recht ein, Daten von Kunden der kostenlosen Version „Antivirus Free" zu verkaufen. „Wir verwenden Daten, um […] Mitteilungen, Angebote und Werbung zu versenden und aus unseren kostenlosen Angeboten durch Nutzung nicht personenbezogener Daten Geld zu verdienen", steht im erneuerten Text. Entsprechende Infos würden an Dritte weitergegeben und gegebenenfalls zusammengefasst oder anonymisiert öffentlich gezeigt. Dazu gehören die mit dem Gerät verbundene Werbe-ID, der Browser- und Suchverlauf einschließlich der Messdaten, der Internetdienstanbieter bzw. das Mobilfunknetz sowie Infos über „Daten, die Sie auf Ihrem Gerät haben und wie sie genutzt werden".

Dass im Browser- und Suchverlauf Daten enthalten sein könnten, mit denen man User identifizieren kann, ist den Verantwortlichen natürlich bewusst. Daher würden diese Infos auch anonymisiert, „wenn wir darauf aufmerksam werden", wie in den Bestimmungen relativierend geschrieben steht.

Äußerst vage liest sich auch die Liste derer, an die Daten weitergegeben werden. Darunter sind mit AVG verbundene, nicht weiter spezifizierte Unternehmen angeführt, außerdem „bestimmte Suchanbieter" und „ausgewählte Vertriebspartner, Händler und andere Geschäftspartner". Von der Datensammelaktion betroffen sind Unternehmensangaben zufolge nur die Nutzer der Gratis-Software, und auch die könnten dem Vorgehen jederzeit widersprechen.

Experten und Nutzer äußern dennoch jede Menge Kritik: Das AVG-Produkt benehme sich wie Spyware (Spionagesoftware), es handle sich um einen unethischen Vertrauensmissbrauch, oder das sei so, als ob der eigene Bodyguard einen beim Duschen filme, heißt es im Netz. Vereinzelt ortet man freilich auch Verständnis; etwa, wenn ein Kommentator schreibt, dass die neue Richtlinie klar und einfach formuliert sei – und dass außerdem eine Unzahl an Softwareanbietern ihre Kundendaten zu Geld machen, die wenigsten jedoch ihre Kunden transparent darüber aufklären.

Auch Avira und Avast verdienen an Userdaten

Tatsächlich ist AVG ja nicht das einzige so agierende Unternehmen aus der Branche. Auch in den Datenschutzrichtlinien von Avira steht geschrieben, dass man die „erhobenen Informationen" dazu verwende, Inhalte anzubieten, die besser auf die Nutzerbedürfnisse zugeschnitten seien – konkret, „damit wir Ihnen treffendere Suchergebnisse und Werbeanzeigen zur Verfügung stellen können […]. Auf diese Weise sind wir in der Lage, unsere Geschäftsaktivi-

Foto Fernrohr: Yurchyks / Shutterstock.com

täten zu unterstützen, damit wir Ihnen auch weiterhin gewisse Produkte kostenlos zur Verfügung stellen können." Weiters informiert das Virenschutz-Unternehmen, dass es gegebenenfalls in der Lage sei, ein persönliches Profil seiner User zu erstellen. Auch in den lediglich in englischer Sprache verfassten Bestimmungen von Avast steht, dass spezielle Firmen damit betraut seien, Werbeanzeigen in den Avast-Anwendungen zu platzieren und dabei anonymisierte Datenprofile von Nutzern anzulegen, um maßgeschneiderte Reklame einblenden zu können.
Kurzum: Die Tatsache, dass kostenlose Angebote im Internet eben nur vermeintlich gratis zu haben sind, in Wahrheit aber mit Daten bezahlt werden müssen, macht auch vor den Virenschutzanbietern nicht halt.

Ärgerliche Zusatzinstallationen

Aber es kommt noch schlimmer. In unserem Test von Internetschutzpaketen in KONSUMENT 5/2015 haben wir nicht nur den Informationsfluss zu Drittanbietern (darunter Google) festgestellt, sondern auch die Tatsache, dass sowohl die kostenlose als auch die kostenpflichtige Schutzsoftware immer öfter Browser-Toolbars und -Erweiterungen mitinstalliert, ungefragt die Suchmaschineneinstellungen ändert oder ähnliche Eingriffe auf dem PC vornimmt.
Ausgerechnet Anbieter von Sicherheitssoftware bauen auf diese Weise potenzielle Schwachstellen in ihre Programme ein. Schon 2013 registrierten wir, dass diverse Virenschutz-Apps für Android-Smartphones unnötigerweise auch die Telefonnummer, die E-Mail-Adresse, Positionsdaten oder eine eindeutige Gerätekennung an die App-Anbieter weiterleiteten.
Zu einem ähnlichen Ergebnis kam im Vorjahr der Heise-Verlag, als er Android-Apps unter die Lupe nahm. Heraus kam, dass vier von sechs Anwendungen ernsthafte Datenlecks im System aufwiesen. Die kostenlosen Produkte von Avast und AVG unterwanderten (so wie auch auch Dr. Web, Lockout und Norton) den verschlüsselten Datenaustausch, weil sie sogenannte Reputationsanfragen im Klartext übermittelten. Mit Reputationsanfragen sind Anfragen zu Internetadressen gemeint, die von den PCs zu den Servern der Antivirenfirmen geschickt werden, damit dort geprüft wird, ob eine Gefahr von ihnen ausgeht. Diese Methode wird beim von vielen Virenschutzprogrammen angebotenen Safe-Browsing eingesetzt. Avast und AVG haben dabei nicht nur die Adressen der Seiten unverschlüsselt in ihre Clouds geschickt, sondern auch URL-Parameter. Das sind jene (hinteren) Bestandteile von Internetadressen, die Informationen über die aktuelle Browsersitzung des Internetnutzers enthalten. In diesen Datensätzen können sich auch Passwörter oder Session-IDs befinden. Infos, mit denen man beispielsweise unter dem Namen anderer Online-Shopping betreiben kann.
Mittlerweile haben Avast und AVG dieses Problem beseitigt, wenngleich nur teilweise und auf unterschiedliche Art und Weise. AVG verzichtet auf die Übertragung der URL-Parameter, überträgt die Reputationsabfragen aber nach wie vor unverschlüsselt. Avast überträgt URL-Parameter zwar weiterhin, schickt die Reputationsabfragen aber nun verschlüsselt ins Netz.
Wir Nutzer bleiben dabei ratlos zurück, denn noch immer gilt, dass der Verzicht auf Virenschutz die schlechteste aller Lösungen ist. Schade, dass seine Verwendung schön langsam zur insgesamt zweitschlechtesten verkommt.

Rat und Hilfe für Verbraucher in Europa ECC-Net
Co-funded by the European Union

Dieser Artikel entstand im Rahmen der „Action 670702 – ECC-NET AT FPA", für welche das Europäische Verbraucherzentrum Österreich Förderungen aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014–2020) erhält.

Mehr zum Thema

Bisher in KONSUMENT erschienen:

Google und der Datenschutz	1/15
Facebook und der Datenschutz	2/15
Amazon und der Datenschutz	3/15
WhatsApp und der Datenschutz	4/15
Mjam und der Datenschutz	5/15
Zalando und der Datenschutz	6/15
PayPal und der Datenschutz	7/15
Freemail-Dienste und der Datenschutz	8/15
Runtastic und der Datenschutz	9/15
Booking.com und der Datenschutz	10/15
Spotify und der Datenschutz	11/15

Virenschutz

Vertrauensbruch

Wir Menschen haben es im Leben gerne übersichtlich und neigen zur Schwarz-Weiß-Malerei. Nach dem einfachen Strickmuster von Hollywood-Actionfilmen teilen wir die Welt in „gut" und „böse" und haben dies auch auf die virtuelle Realität des Internets übertragen. Und dann erfahren wir, dass AVG und andere Virenschutzanbieter, die bisher eindeutig zu den „Guten" zählten, die Daten der Nutzer ihrer kostenlosen Virenscanner an die Werbewirtschaft und andere Dritte verkaufen. Anders lasse sich der Fortbestand der Gratis-Software nicht mehr finanzieren, so wird argumentiert.

Gernot Schönfeldinger
Redakteur
gschoenfeldinger@vki.at

Plötzlich gibt es da einen grauen Fleck in unserem Weltbild, den wir irgendwo zwischen Schwarz und Weiß einordnen müssen. Ehrlicherweise ist es nicht der einzige graue Fleck, mit dem wir konfrontiert sind. Aber es ist ein irritierender und schmerzlicher, weil Virenschutzanbieter höchstes Vertrauen genießen. Kaum einer anderen Drittanbieter-Software gewähren wir so bedenkenlos umfassenden Zugriff auf unsere PCs und Smartphones.
Der Datenverkauf ist daher keine lässliche Sünde, so wie bei Facebook oder Google – jenen Datenkraken, die wir schicksalsergeben als „eh noch die Besseren unter den Bösen" einstufen, weil wir ihren praktischen Nutzen schätzen. Es handelt sich um den kaum wiedergutzumachenden Sündenfall des Vertrauensbruchs. Natürlich ist da noch die Sache mit dem geschenkten Gaul. Nur gab es in früheren Jahren ja gar keinen Anlass, ihm ins Maul zu schauen. Vielleicht wäre es für alle Beteiligten hilfreicher gewesen, die Gratisversionen rechtzeitig einzumotten?
Schutzpakete gegen Schadsoftware sind nicht perfekt, doch im Großen und Ganzen nützlich und dahinter steckt viel Arbeit. Es geht schon in Ordnung, die erbrachte Leistung mit einem angemessenen Betrag zu honorieren. Aber leider sind mittlerweile auch die kommerziellen Versionen unter Verdacht geraten. Ein grauer Schleier hat sich über das Weiß gelegt. Wem können wir am Ende des Tages überhaupt noch vertrauen? Die Kategorie „die Böseren unter den Guten" hatten wir in unserem schwarz-weißen Weltbild eigentlich nicht vorgesehen.

Foto Dartpfeil: Ljupco Smokovski / Shutterstock.com