Virenschutz ≠ Datenschutz

Wie Avast die Daten seiner Kunden verkaufte

„Jede Suche. Jeder Klick. Jeder Einkauf. Auf jeder Website." So pries der Virenschutz-Anbieter Avast die Surfdaten seiner Kunden an. Mit dem Verkauf der Daten hat das Unternehmen jahrelang Millionen verdient. c't hat einen Blick in die angeblich anonymisierten Datenpakete geworfen.

Von Ronald Eikenberg

Etwa 435 Millionen Nutzer vertrauen der Virenschutz-Software des tschechischen AV-Herstellers Avast, wenn man den Angaben des Herstellers glaubt. Das Unternehmen steckt nicht nur hinter dem gleichnamigen Virenschutz, es hat sich auch die Antivirenfirma AVG sowie den populären System-Cleaner CCleaner einverleibt. Die Produkte sind auch deshalb so beliebt, weil man sie kostenlos nutzen kann. Die Gratisversionen machen Werbung für die kostenpflichtigen Produkte von Avast – doch das ist nicht die einzige Einnahmequelle: Avast hat umfangreiche Daten über das Surfverhalten seiner Nutzer erfasst und verkauft: „Examine every search, click, and buy. On every site.", hieß es auf der Website der mehrheitlich zu Avast gehörigen Firma Jumpshot.

Der Name Jumpshot dürfe den wenigsten Avast-Nutzern ein Begriff gewesen sein, denn die Tochterfirma hatte Ihr Angebot auf Unternehmenskunden ausgerichtet. In einer Pressemitteilung aus dem Juli 2019 nennt Jumpshot unter anderem Microsoft, Google, Yelp und TripAdvisor als seine Kunden. Das Unternehmen wirbt in der Mitteilung damit, täglich fünf Milliarden Nutzeraktionen zu tracken – und zwar in Echtzeit. Laut einem Bericht des Online-Magazins Motherboard hat eine Marketingfirma im Jahr 2019 über zwei Millionen US-Dollar gezahlt, um auf die wertvollen Daten zugreifen zu dürfen. Das Geschäft mit den Kundendaten war offenbar äußerst lukrativ.

Den Anfang nahm die Geschichte vor rund sieben Jahren: Im September 2013 gab Avast bekannt, ein Unternehmen namens Jumpshot übernommen zu haben, das damals eine Tune-up-Software herausgegeben hatte. Daraufhin hat sich die Ausrichtung des Neuzugangs offenbar geändert. Im Mai 2015 bezeichnete Avast in seinem Blog Jumpshot als „Marketing Analytics Company" und warb mit „einzigartigen Einblicken" in das Kaufverhalten von Online-Shoppern. Schon damals machte der Virenschutz-Anbieter kein Geheimnis daraus, dass diese Einblicke aus den Daten der Avast-Nutzer generiert werden. Das Unternehmen versicherte jedoch, dass die Avast-Server keine Daten verlassen, die sich zur Identifizierung einzelner Nutzer eignen. Dies solle ein Algorithmus sicherstellen, den sich Jumpshot patentieren ließ.

Patentierter Datenschutz?

Einen Tag nach dem Blogpost lieferte Ondřej Vlček, damals Leiter der Abteilung „Consumer Business" bei Avast, im Unternehmensforum Details zu den Daten, die weitergegeben werden sollen, und zu dem Algorithmus, der die brisanten Bestandteile herausfiltern soll. Die Daten umfassen demnach unter anderem die URL und den Referer, also die Adresse der Website, über die ein Nutzer auf die angesteuerte Seite gelangt ist. Der große Aufschrei blieb damals aus, der Forenbeitrag wurde nur von einer Handvoll Nutzer kommentiert.

Das Thema Jumpshot geriet in Vergessenheit und Avast machte mit anderen Themen Schlagzeilen. So wurde im September 2017 bekannt, dass Cyber-Ganoven das Aufräumprogramm CCleaner missbrauchten, um gezielt Schadsoftware zu verteilen. Im Oktober 2019 erklärte Avast, dass Angreifer durch einen vergessenen VPN-Zugang fast ein halbes Jahr auf das Unternehmensnetz zugreifen konnten.

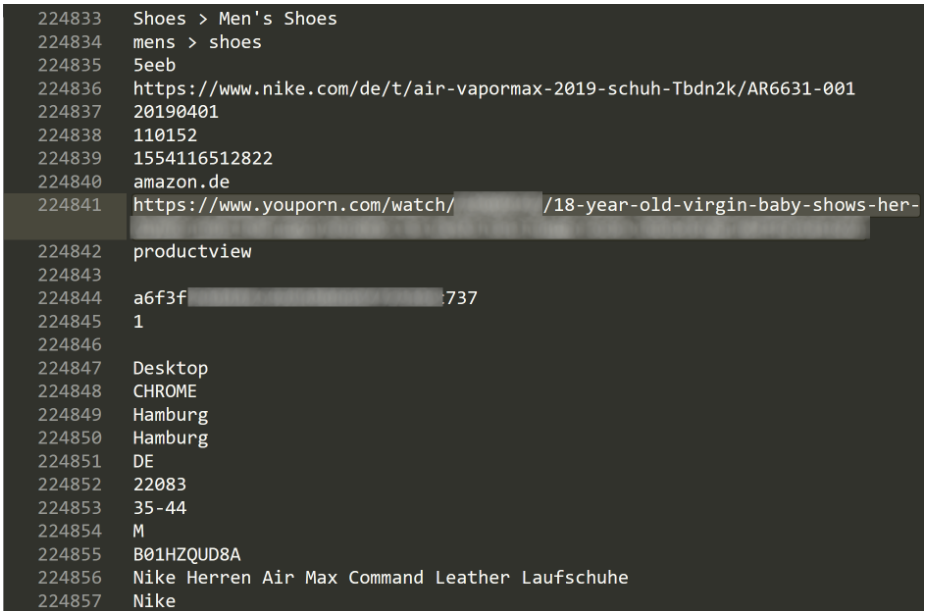
Wenige Tage später berichtete der Sicherheitsforscher Wladimir Palant in seinem Blog von einem auffälligen Datenabfluss bei Nutzung der Browser-Erweiterungen von Avast und brachte damit die Marketing-Maschine Jumpshot unbewusst wieder aufs Tapet. Er bemerkte, dass Browser-Erweiterungen von Avast und AVG sowohl beim Surfen als auch beim Wechseln zwischen Tabs die vollständige URL der angesteuerten Webseiten an den Avast-Server uib.ff.avast.com schickten. Zudem wurden laut Palant unter anderem auch Seitentitel, Referer, Sprache und Ländercode des Nutzers sowie eine Nutzer-ID übertragen. Google, Opera und Mozilla entfernten die Erweiterungen daraufhin größtenteils aus den Add-on-Stores, während der Avast-CEO in einem Forbes-Interview die Datensammelpraxis verteidigte.

Wirklich anonym?

Doch damit war das Thema noch nicht vom Tisch. Die Online-Magazine Motherboard

Der Gratis-Virenschutz Avast hat Daten über das Surfverhalten seiner Nutzer weitergegeben.

und PCMag haben sich daraufhin intensiv mit dem Datendealer Jumpshot befasst und die Effektivität der Datenanonymisierung infrage gestellt. Auch eine Analyse von c't weckt Zweifel daran, dass die Identitäten der Avast-Nutzer ausreichend gut geschützt wurden. Uns wurde ein 18 GByte großes Datenpaket zugespielt, das augenscheinlich von Jumpshot stammt. Bei der Sichtung sind uns nicht nur potenziell kritische URL-Parameter aufgefallen, etwa Session-IDs für Webmail-Dienste wie GMX, sondern auch Zugriffe auf Dokumente, anhand derer man den Personenkreis zumindest eingrenzen kann, zum Beispiel ein Studienplan der Technischen Universität Dresden. Ein anderes PDF-Dokument ist offenbar auf einem SharePoint-Server gespeichert, der nicht öffentlich zugänglich ist. Anhand der URL kann man hier nicht nur auf den Inhalt des Dokuments schließen, sondern auch auf den Betreiber der SharePoint-Instanz, eine Ausbildungsstätte für Pastoren und Prediger.



Intime Einblicke: Dieser Avast-Nutzer aus Hamburg interessiert sich offenbar nicht nur für Nike-Schuhe, sondern auch für Pornos.

In den Daten stießen wir auch auf allerhand Pikantes, darunter etliche Aufrufe von Pornoseiten mit sprechenden URLs, durch die man auf die sexuellen Vorlieben der Avast-Nutzer schließen kann. Warum diese Adressen in ein Datenpaket gelangt sind, das Jumpshot offenbar zum Thema „Online Schuhe kaufen" geschnürt hatte, konnten wir nicht nachvollziehen. Auch ein Swingerportal ist mehrfach vertreten. Die Aufrufe in den Datenpaketen sind offenbar mit Nutzer-IDs versehen, die sich zwar nicht direkt einer Person zuordnen lassen. Wer jedoch Zugriff auf einen der Server hat, die in den Jumpshot-Daten auftauchen, kann diese anhand der Zeitstempel vermutlich mit seinen Server-Logs abgleichen und so die IDs einzelnen Personen zuordnen. Anschließend ließe sich das Surfverhalten dieser Personen auch auf anderen Sites nachvollziehen.

Auf die jüngsten Berichte über Jumpshot folgte ein internationales Medienecho, das Avast schließlich nicht mehr ignorieren konnte. Ende Januar gab Ondřej Vlček, inzwischen zum Avast-CEO aufgestiegen, bekannt, dass Jumpshot ab sofort Geschichte sei. Die Datensammelei werde umgehend eingestellt und das Unternehmen abgewickelt. Mit dieser Nachricht wurde auch das Ausmaß bekannt, das der Datenhandel inzwischen angenommen hatte: Laut Vlček sind von der Jumpshot-Schließung hunderte Mitarbeiter betroffen.

Ob die Eliminierung von Jumpshot hilft, das Vertrauen der Kunden zurückzugewinnen, ist fraglich. Insbesondere bei Virenschutzsoftware ist Vertrauen gegenüber dem Hersteller unerlässlich, denn solche Programme klinken sich prinzipbedingt sehr tief ins System ein. Auch ein kontinuierlicher Datenaustausch mit der Hersteller-Cloud ist fester Bestandteil moderner Schutzprogramme. Was mit den Daten geschieht, kann der Nutzer nicht überprüfen. Man sollte sich die Frage stellen, ob die Installation eines Antivirenprogramm überhaupt noch sein muss – denn der seit Windows 8 vorinstallierte Defender schneidet in den Vergleichstests der AV-Testlabore seit geraumer Zeit gut ab. *(rei@ct.de)* c't