Spione, die Spione jagen

Eben war Jewgeni Kasperski ein weltweit anerkannter Virenjäger. Plötzlich galt er als russischer Spion. Nun ist er vor wenigen Monaten mit einigen Servern nach Zürich umgezogen. Was steckt hinter all dem? Und was bedeutet das für unser aller Privatsphäre?

Von Eva Wolfangel, 07.02.2019

Viren haben ihn berühmt und wohlhabend gemacht. Jetzt steht er unter einem bösen Verdacht: Jewgeni Kasperski. Pavel Golovkin/AP Photo

Früher wäre es recht aufwendig gewesen, Sie zu überwachen. Agenten hätten heimlich die Fenster oder Türen Ihrer Wohnung aufbrechen müssen, hätten Wanzen und Kameras installieren und sich im Haus gegenüber einmieten müssen, hätten Schichtdienst leisten müssen, um Sie zu observieren.

Heute ist es ziemlich einfach: Es genügt, wenn die Agenten Ihren Computer oder Ihr Smartphone hacken.

Etwa, indem sie Ihre Antiviren-Software manipulieren, jenes Programm, das Sie eigentlich schützen soll. Und das sich am besten eignet für einen Angriff auf Ihre Privatsphäre. Weil diese Programme alles dürfen: Sich in

den tiefsten Tiefen Ihrer Festplatten umsehen, alles verändern, beliebig viele Daten herauf- und herunterladen.

Gelingt es jemandem, eine Antiviren-Software zu manipulieren – dann werden Millionen Computer zu Wanzen.

Und die Frage ist: Hat Jewgeni Kasperski, Gründer von Kaspersky Lab und ein weltweit bekannter Virenjäger, gemeinsame Sache gemacht mit dem russischen Geheimdienst, um genau das zu tun: Computer in Spionagewerkzeuge zu verwandeln?

Der Verdacht steht im Raum. Bewiesen ist nichts. So oder so, hier vorab ein Tipp: Ganz egal, ob Sie eine Antiviren-Software amerikanischer, russischer oder chinesischer Herkunft nutzen, es gibt gute Gründe, darauf zu verzichten.

Wer ist Kasperski?

Geheimdienste und Virenjäger sind natürliche Feinde. Virenjäger wollen Sicherheitslücken in Programmen schliessen, damit Agenten und Einbrecher nicht ohne weiteres in private Rechner eindringen können.

Geheimdienste wollen ausgewählte Sicherheitslücken möglichst lange offen halten, um ungehindert auf privaten Rechnern herumschnüffeln zu können.

Und der schlaue Kasperski und seine Leute haben den Hackern des amerikanischen NSA, des russischen FSB und des israelischen Mossad wiederholt die Türen ihrer schönsten Geheimgänge vor der Nase zugeworfen.

Ist das ganze Theater nur eine Finte der Geheimdienste, um Kasperski aus dem Spiel zu nehmen? Denkbar ist es.

Als Schüler galt er als Wunderkind. Mit 15 belegte Jewgeni Kasperski den zweiten Platz eines Russland-weiten Mathematikwettbewerbs, kurz darauf schrieb er sein erstes Computerprogramm, später studierte er an der KGB-Hochschule für Mathematik, Kryptografie und Computertechnologie in Moskau.

1997 gründete Jewgeni Kasperski gemeinsam mit seiner ersten Frau Natalja das Kaspersky Lab, und spätestens damit zählten sie und ihre Kollegen zu den besten Spürhunden im Internet. 2010 halfen sie, den Sabotage-Wurm Stuxnet zu enttarnen, der mutmasslich allein dafür programmiert worden war, um das iranische Atomprogramm zu sabotieren – der aber auch andere Infrastruktur bedrohte.

Zugleich ist Jewgeni Kasperski ein Lebemann. Er hat eine Jacht und fährt einen Ferrari, sponsert Autorennen und reist gern um die Welt. Er ist ein beliebter Vortragsredner, weil er sich auskennt und auch mal einen Witz reisst. Er weiss, wie allgegenwärtig Spione sind: Meist benutzt er ein Uralt-Handy, ohne GPS oder Datenzugang.

2017 machte Kaspersky Lab einen Umsatz von knapp 700 Millionen US-Dollar. Und auch wenn die Firma inzwischen weltweit mehr als 3800-Menschen beschäftigt, lebt sie bis heute vom genialischen Ruf ihres Gründers, der immer wieder medienwirksam vor Viren, Würmern und sonstigem Ungeziefer warnt – jenem Gewürm, mit deren Bekämpfung die Firma viel Geld verdient.

Dann geriet alles ins Rutschen. Als sein Lab attackiert wurde und plötzlich die Frage im Raum stand: Macht er seit langem gemeinsame Sache mit dem russischen Geheimdienst?

Die Zürich-Show

Seit November 2018 stehen die Server, auf denen Kaspersky die europäischen Kundenanfragen verarbeitet, in Zürich-Glattbrugg, in einem dreistöckigen Flachbau. Das Lab hat sich bei Interxion eingemietet, einem niederländischen Anbieter, der in Europa 50 Rechenzentren betreibt, eines davon in der Schweiz.

Dort sieht es aus wie überall, wo grosse Mengen an Daten gespeichert und verarbeitet werden: lange Flure, blinkende Serverschränke, eine laut summende Klimaanlage, unzählige Sicherheitsschleusen, Sprinkleranlagen.

Im Juni 2018 fuhren hier Panzer vor, die Schweizer Armee überwachte das Rechenzentrum eine knappe Woche lang, man probte den Ernstfall: Wie könnte kritische Infrastruktur bei einer Krise geschützt werden? Das Rechenzentrum gehört offenbar dazu.

Das Kalkül von Kaspersky: Neutralität demonstrieren. Der Öffentlichkeit zeigen, dass seine Firma weit weg ist vom Kreml. Und sei es, indem sie einen Teil ihrer Daten in Zürich hostet, in der neutralen Schweiz, wo Datenschutz hohe Priorität geniesst.

Das ist zu einem guten Teil Show. Denn natürlich können auch die russischen Kaspersky-Mitarbeiter auf die Server in der Schweiz zugreifen, um Virendatenbanken abzugleichen. Anders ginge es gar nicht. Viren kennen keine Grenzen. Und das muss dann eben auch für Virenjäger gelten.

Wäre es nicht eine Lösung, ganz in die Schweiz umzuziehen und Moskau endgültig den Rücken zu kehren? Darauf gab Kasperski an der Pressekonferenz, an der er seine «Transparenzinitiative» vorstellte, eine verblüffend einfache Antwort: Würde er gern, aber das ist zu teuer.

Kasperski: «Für das Gehalt, das ein Softwareentwickler in der Schweiz verlangt, können Sie in Russland fünf Entwickler anstellen.»

Digitale Fingerabdrücke

Der Spionagefall, der Kaspersky beinahe seinen guten Ruf kostet, ist verwickelt und in seinen Details für Laien kaum nachzuvollziehen. Bereits 2014 gelang es Hackern des israelischen Geheimdienstes offenbar, sich im Inneren der Kaspersky-Server umzusehen. Dabei wollen sie entdeckt haben, dass das Lab gerade dabei war, dem amerikanischen Geheimdienst NSA hinterherzuschnüffeln und dessen Spionage-Werkzeuge zu enttarnen – im Auftrag des russischen Geheimdienstes FSB.

Als sich die Spione begegneten, zwischen den Codezeilen irgendwelcher Programme, bemerkten das zunächst nur die israelischen Hacker.

Die russischen Hacker hingegen hatten sich offenbar unbeobachtet gewähnt und ungeniert nach Codenamen von NSA-Operationen gesucht. Sie nutzten dafür – so der Bericht der Israelis – Kasperskys Antiviren-Software.

Erst im Frühjahr 2015 entdeckten die Kaspersky-Leute die Spuren der israelischen Spione. Was aus den Veröffentlichungen des Labs darüber deutlich wird: Es war ein Angriff, der selbst für Profis kaum zu entdecken ist. In

Hacker-Foren wird bis heute gerätselt, wie Kaspersky und seine Kolleginnen diese perfekt verwischten Spuren überhaupt haben entdecken können. Niemand kann sich besser tarnen als Hacker in Diensten der Geheimdienste – und der israelische Geheimdienst gilt als einer der besten der digitalen Welt.

Später verpetzten die israelischen Hacker Kaspersky in den USA und berichteten US-Politikern von dessen Schnüffelei, in einer nicht öffentlichen Aussprache. Alle Beteiligten weigern sich danach, Journalisten Beweise jedweder Art zu zeigen.

Erst am 5. Oktober 2017 wurde öffentlich, was die israelischen Staatshacker auf den Kaspersky-Servern entdeckt haben wollen.

Schlagartig stand der Vorwurf im Raum: Das Kaspersky Lab habe in seine Antiviren-Programme einen Mechanismus eingebaut, über den der russische Geheimdienst Daten abzapfen kann. Damit wären 400 Millionen Computer in aller Welt, auf denen die Software läuft, theoretisch russische Wanzen.

Nur Tage später ordnete die US-Regierung an, alle Kaspersky-Programme von allen Behördenrechnern zu löschen. Dem Lab sei nicht zu trauen.

Im Juni 2018 zog Europa nach. Das EU-Parlament verabschiedete einen Entwurf zur Cyberabwehr und führte darin das Kaspersky Lab unter «als böswillig eingestufte Programme und Geräte» auf. Das EU-Parlament empfahl ein Verbot der Software für Behörden und staatliche Stellen.

Die Schlagzeilen verunsicherten viele Kunden. Zwar gehören die Antiviren-Programme von Kaspersky immer noch zu den besten und landen bei Tests regelmässig auf dem Siegerpodest. Aber die Anschuldigungen kostete die Firma viele Kunden. Wobei – laut Kaspersky – die Umsätze insgesamt nicht zurückgehen: Was man im Westen verliere, gewinne man gerade in China zurück. Nach dem Motto: Der Feind meines Feindes ist mein Freund.

«Unsere Software ist missbraucht worden»

Es dauert, bis sich ein Firmenvertreter äussert. Erst nach zwei Monaten und einigen Nachfragen kommt endlich ein Telefoninterview zustande mit Anton Schingarew, einem Sprecher des Unternehmens. Schingarew ist bester Laune, auskunftsfreudig und höflich. Ein Gespräch via Skype hat er abgelehnt, er will nur verschlüsselt kommunizieren, via Facetime, Whatsapp oder Threema. Obwohl er in Moskau sitzt, ist er unter einer amerikanischen Handynummer zu erreichen. Er sei viel unterwegs, sagt er ausweichend auf die Nachfrage dazu.

Also sprechen wir per Threema – Schingarew lobt den Schweizer Messenger-Dienst ausgiebig als «eine sehr sichere App».

Herr Schingarew, hat die Firma Kaspersky Lab für den russischen Geheimdienst spioniert?
Wir haben von den Vorwürfen gehört, aber keiner der Beteiligten hat uns je kontaktiert – trotz mehrmaliger Einladung. Wir haben keinen einzigen Beweis gesehen, kein einziges Dokument. Wir würden gerne verstehen und aufklären, in welcher Form unsere Software eingesetzt wurde, aber man gibt uns diese Gelegenheit nicht.

Können Sie ausschliessen, dass der Vorfall stattgefunden hat?
Ich bin mir sicher, dass unsere Firma nicht selbst spioniert hat. Das wäre

Selbstmord. Wenn, dann ist unsere Software missbraucht worden – ohne das Wissen oder das Zutun unseres Unternehmens.

Die «New York Times» schreibt, Ihre Software sei «wie eine Googlesuche für sensible Informationen» benutzt worden. Für den russischen Geheimdienst wäre so eine Suche auf amerikanischen Geheimdienst-Rechnern ein Traum.
Das ist technisch plausibel, aber wir arbeiten nicht für den russischen Geheimdienst. Es ist unsere Aufgabe, Spione zu enttarnen. Unsere Technologie ist eine der besten in diesem Zusammenhang. Das macht manche Regierungen wütend.

Wie können wir da sicher sein? Der Gründer des Messenger-Dienstes Telegram ist aus Russland geflohen, weil ein Gericht ihn zwingen wollte, Hintertüren für den russischen Geheimdienst FSB einzubauen. Worauf der Dienst von den Behörden blockiert wurde. Sie aber sitzen weiterhin unbehelligt in Russland, und Ihr Gründer Jewgeni Kasperski hat alle Freiheiten. Wie passt das zusammen?
Bei Telegram ging es darum, einen Schlüssel zur Verfügung zu stellen, um verschlüsselte Nachrichten lesen zu können – das ist in Russland für Telekommunikationsanbieter gesetzlich vorgeschrieben. Andere Messenger-Apps haben das gleiche Problem. Aber es gibt kein Gesetz, das vorschreibt, dass Antiviren-Programm-Anbieter Hintertüren für Behörden einbauen müssten.

Hat der russische Geheimdienst Ihre Firma jemals kontaktiert mit der Bitte, für ihn zu spionieren?
Sollte es eine solche Anfrage geben, werden wir uns weigern, ihr nachzukommen. Jewgeni Kasperski hat öffentlich klargemacht: Sollten wir je gezwungen werden, Hintertüren für Behörden einzubauen, werden wir Russland verlassen.

Weshalb verlassen Sie Russland nicht jetzt schon komplett? Wäre das nicht der einfachste Weg, das Vertrauen in Ihr Unternehmen wieder herzustellen?
Wir werden das tun, sobald es Druck seitens der Behörden gibt. Aber den gibt es derzeit nicht. Im Augenblick dreht sich alles um Politik, vor dem Hintergrund der Spannungen zwischen Russland und den USA. Wir sind ein Unternehmen, das leicht zu beschuldigen ist. Bis vor kurzem hat man uns noch vertraut, und plötzlich soll alles anders sein? Und wir bekommen keine Details genannt. Das ist unfair.

Ein Hacker spricht

Fragen wir einen erfahrenen *white hacker,* was er von der Sache hält. Der Mann attackiert im Auftrag von Konzernen deren Server und Netzwerke, um mögliche Schwachstellen zu entdecken.

Er tut dann so, als sei er ein echter, «böser» Hacker. Und zeigt den Unternehmen später, wie sie sich besser schützen müssen. Er sagt von sich: «Ich und meine Kollegen kommen überall rein.»

Weil er weiss, was technisch möglich ist, ist er immer sehr, sehr vorsichtig: Auf Reisen in die USA und nach Russland nimmt er stets leere Laptops und Smartphones mit und entsorgt sie, falls er sie einem Grenzbeamten aushändigen musste. Und er nutzt selbst nie Antiviren-Software. Zu riskant.

«Wenn ich was zu sagen hätte im russischen Geheimdienst, würde ich das genau so machen», sagt der Mann, der anonym bleiben möchte. Er würde

viel Energie und Geld investieren, um Jewgeni Kasperski auf seine Seite zu ziehen. Weil es kaum einen effizienteren Weg in die Rechner dieser Welt gebe als über deren Antiviren-Software.

Er misstraue Kaspersky genauso wie Antiviren-Firmen aus den USA. «Da gibt es keinen grossen Unterschied zwischen russischen und amerikanischen Anbietern», sagt er. «Bei beiden besteht die Gefahr, dass sie ihrer Regierung zuarbeiten.»

Schuldig oder unschuldig?

Niemand kann es mit Sicherheit sagen. Es gibt in der Welt der Codezeilen und Hackerangriffe meist nur Indizien, keine Beweise. Fünf Gründe sprechen für Kaspersky:

1. **Es fehlen weiterhin Beweise.** Die Recherchen des EU-Parlaments laufen auf die Aussage heraus: Man könne nicht beweisen, dass Kaspersky es *nicht* tut. In einer Antwort auf eine parlamentarische Anfrage, inwiefern Kaspersky-Software von EU-Behörden genutzt worden sei, heisst es: «Die Kommission hat jedoch keine Hinweise auf eine Gefahr, die mit dieser Antiviren-Software verbunden ist.»
2. **Die Firma will weiter Transparenz üben.** Im Republik-Interview sagte der Sprecher, dass Kaspersky Lab den Quellcode ihrer Software einschliesslich aller Updates gegenüber neutralen Organisationen offenlegen will, um sie unabhängig überprüfen zu lassen. Balthasar Glättli, grüner Nationalrat und Mitglied der Sicherheitspolitischen Kommission, ist überrascht: «Von einem solchen Angebot höre ich durch Ihre Anfrage zum ersten Mal.» Den Vorstoss begrüsst er allerdings: «Gerade bei sicherheitsrelevanter Software wäre grundsätzlich die Veröffentlichung des Quellcodes die geeignetste Massnahme, um den Verdacht auf Hintertüren oder Sicherheitslücken ausschliessen zu können.»
3. Apropos Hacker: Noch sicherer wäre es, wenn Kaspersky den Code frei zugänglich machen würde. Gäbe es darin verräterische Elemente, würde ein Hacker oder ein Computer-Sicherheitsforscher ihn früher oder später entdecken, schliesslich kann er sich mit solchen Funden profilieren. Aber auch so – **bislang hat kein Hacker verräterische Spuren in der Software von Kaspersky entdeckt,** und sie können sich schliesslich auch auf andere Weise Zugang zu Systemen verschaffen. Es bleibt einzig die mysteriöse Aussage der israelischen Geheimdienstler, die nicht unabhängig überprüft werden kann.
4. **Die Firma hat in der Vergangenheit gegen Geheimdienste gearbeitet,** der Gründer vertritt diese Position glaubhaft. Für den amerikanischen Geheimdienst ist Kaspersky ein starker Gegner. Es ist naheliegend, dass die NSA jede Gelegenheit nutzt, um Kaspersky zu schaden. Das Leben der Spione wäre einfacher ohne Kaspersky.
5. Vor einigen Tagen kam ans Licht, dass Kaspersky der NSA aus der Patsche geholfen hat – und ihnen half, einen Maulwurf zu verhaften. Wie zwei ungenannte Personen dem Magazin «Politico» verrieten, hatte ein NSA-Mitarbeiter über zwei Jahrzehnte hinweg streng geheime Unterlagen seines Arbeitgebers kopiert: 50 Terabyte Daten, darunter teils die raffiniertesten Hacking-Werkzeuge des Geheimdienstes – und sie im August 2016 öffentlich feilgeboten. **Mitarbeiter von Kasperski entarnten den Mann und gaben dem US-Geheimdienst einen entsprechenden Tipp** – sodass besagter Harold T. Martin am 27. August 2016 verhaftet wurde.

Wobei: Das alles ist auch kein Beweis für Kasperskys Unschuld.

Die Spione sind überall

Wir alle können getrost davon ausgehen, dass Geheimdienste auf unseren Rechnern unterwegs sind. Nicht, weil man uns zutraut, ein grosses Ding drehen oder die öffentliche Ordnung stören zu wollen, sondern aus Prinzip. Weil Geheimdienste grundsätzlich so viele Daten wie möglich sammeln; wer weiss, wofür man sie eines Tages gebrauchen kann.

Ihr Credo: Eine perfekte, lückenlose Überwachung macht die Welt sicherer.

Das ist kein Verfolgungswahn. Das haben die Enthüllungen Edward Snowdens gezeigt. Einmal hatte die Welt Einblick in die radikale Sammelwut der Geheimdienste. Für sie ist Privatsphäre kein Wert, sondern ein Risiko.

Nach den Enthüllungen Snowdens herrschte in der Hackerszene Genugtuung: Sie hatten es geahnt, man hatte es ihnen nicht geglaubt. Und einmal mehr war klar: Was immer technisch möglich ist, wird gemacht.

Was folgt daraus für Privatnutzer? Vor allem: auf aktuelle Software zu setzen und sein Betriebssystem und seinen Browser ständig zu aktualisieren. Wer Windows 10 oder macOS Mojave nutzt, kann zusätzliche Antiviren-Software getrost in den Müll werfen, ganz egal, ob sie amerikanischer, russischer oder chinesischer Herkunft ist. Wer seinen Rechner regelmässig aktualisiert und die üblichen Vorsichtsmassnahmen berücksichtigt, ist gut abgesichert.

Noch etwas folgt aus dem Fall Kaspersky: Technisch ist der Kampf gegen die staatlichen Schnüffler nicht zu gewinnen. Es ist ein politischer Kampf. Nur Staaten können die Daten saugenden Sicherheitsfanatiker aufhalten.

Die Recherche

Als Wissenschaftsautorin Eva Wolfangel vom Fall Kaspersky hörte, hätte sie gern jemanden interviewt, der den Virenjäger seit langem persönlich kennt. Aber so jemanden fand sie nicht. Also recherchierte sie vor allem in der Hackerszene in Deutschland und der Schweiz. Einen Tag verbrachte sie mit einem *white hacker* und sah ihm über die Schulter, wie er einen Konzern attackierte – im Auftrag dieses Konzerns. Danach war sie ernüchtert. Sie hatte begriffen: Wenn jemand deine Daten will, dann kriegt er sie. Es gibt immer ein Schlupfloch.

Als sie ihr Smartphone im Büro des *white hacker* kurz aus den Augen liess, sagte der ihr: Er würde das Gerät nicht mehr benutzen, wenn ihm das passiert wäre. Wolfangel hat nicht auf seinen Rat gehört.