17.03.2022 | IT-SICHERHEIT

Ist Kaspersky wirklich ein Problem?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor dem russischen Unternehmen. Doch wie berechtigt es ist, Kaspersky als unsicher zu bezeichnen, bleibt unklar.

von Eva Wolfangel

© VLADIMIR GERDO / TASS / DPA / PICTURE ALLIANCE (AUSSCHNITT)

Das Bundesamt für Sicherheit in der Informationstechnik hat davor gewarnt, Softwareprodukte des russischen IT-Sicherheitsunternehmen Kaspersky zu verwenden. Über Kaspersky gab es immer mal wieder Diskussionen – zuletzt

2017, als die US-Regierung es untersagte, Kaspersky-Software in Behörden einzusetzen. Die Begründung damals: Die russischen Geheimdienste seien per Gesetz dazu ermächtigt, Kaspersky zur Unterstützung ihrer Arbeit zu zwingen. Kaspersky selbst widersprach dem umgehend: Das entsprechende Gesetz gelte für Telekommunikationsdienstleister, nicht für Sicherheitsunternehmen. Und Kaspersky spioniere selbstverständlich nicht für die russische Regierung.

Das deutsche BSI vertraute dem Unternehmen damals noch und gab an, es sehe keinen Grund, Kaspersky zu misstrauen: Die Behörde lobte sogar gegenüber der Nachrichtenagentur dpa die seit Jahren gute und »vertrauensvolle Zusammenarbeit« mit Kaspersky. »Das BSI weiß die Zusammenarbeit und die hochwertigen Analysen von Kaspersky zu schätzen«, so die Behörde damals. »Kaspersky Lab hat sich in verschiedenen Fällen als verlässlicher und kompetenter Partner erwiesen.« Es gebe auch keinen Anlass zu vermuten, dass Kaspersky russische Cyberaktivitäten bewusst ignorieren würde. Eine Reihe wichtiger russischer Cyberspionagekampagnen habe das Unternehmen vielmehr als Erstes veröffentlicht und detailliert beschrieben.

Wie es nun zur Änderung der Einschätzung kommt und ob es neue technische Erkenntnisse gibt, auf der die aktuelle Warnung beruht, dazu äußert sich das BSI auf Anfrage nicht. Kaspersky selbst betont, diesbezüglich ebenfalls keine Information bekommen zu haben und bezeichnet die Entscheidung als »politisch«. Jochen Michels, Head of Public Affairs Europe bei Kaspersky, klagt in einem Schreiben an das BSI, das der Autorin vorliegt, von der deutschen Behörde zu wenig Zeit eingeräumt bekommen zu haben, um zu reagieren. Zudem versucht das Unternehmen in dem Schreiben, die Bedenken zu entkräften.

Nachvollziehbare Bedenken

Das BSI warnt unter anderem vor dem Risiko, das allein dadurch entstehe, dass ein Virenscanner weitgehende Systemrechte habe, was Manipulation und Missbrauch durch Kaspersky und/oder Dritte ermögliche. Das allerdings gelte nicht nur für Kaspersky-Software, so Kaspersky, »sondern für alle auf dem Markt befindlichen Antivirenprogramme.« Das stimmt: Antivirenprogramme haben weit gehende Rechte – Nutzenden bleibt nichts anderes übrig, als einen Anbieter zu wählen, dem sie vertrauen, oder sich anderweitig zu schützen.

Dabei könne man die politischen Bedenken im Zusammenhang mit dem Krieg in der Ukraine »sehr gut nachvollziehen«, schreibt Michels. »Ungeachtet der politischen Risiken liegt jedoch der einzige objektive Weg, diesen Risiken zu begegnen, in der Technologie, ihrer Transparenz und anerkannten Validierungsmaßnahmen.« Dafür setze sich Kaspersky ebenso wie das BSI seit Jahren ein. Michels bittet um »eine faktenbasierte Entscheidung.« Inwiefern es einen weiteren Austausch mit Kaspersky gebe, dazu wollte sich ein Sprecher des BSI nicht äußern. Wenn, dann geschehe dies auf vertraulicher Basis. Das BSI habe Kaspersky zudem – der gesetzlichen Vorgabe folgend – »vor Veröffentlichung der Warnung informiert und Gelegenheit zur Stellungnahme gegeben«.

Das Risiko staatlicher Eingriffe durch die russische Regierung sei bei Kaspersky »deutlich geringer als bei allen anderen Cybersicherheitsunternehmen der Welt«, behauptet Michels in seinem Schreiben an das BSI weiter. Schließlich gebe es technische ebenso wie organisatorische Maßnahmen zur Verbesserung der Transparenz und Sicherheit, »die kontinuierlich von anerkannten Organisationen geprüft und zertifiziert werden«.

In der Tat bietet Kaspersky unter anderem unabhängigen Stellen

Einblick in den Quellcode an und lädt in dem Schreiben auch das BSI ein, die Maßnahmen gegen eine Manipulation der Software in den so genannten Transparenzzentren des Unternehmens selbst zu überprüfen. Ein offener Quellcode erhöht zwar die Chance, dass unabhängige Forschende mögliche Hintertüren entdecken, es ist aber natürlich angesichts von Millionen Zeilen von Code auch nicht einfach, diese zu finden. Die Offenheit des Unternehmens ist noch keine Garantie dafür, dass keine Hintertüren existieren. Allerdings hat sich Kaspersky in der Vergangenheit viele Feinde gemacht, weil das Unternehmen mehrere staatliche Spähmissionen aufdeckte und damit deren teure Cyberwaffen nutzlos machte. Von daher bekommt die Software vermutlich schon große Aufmerksamkeit – nämlich von den betroffenen Staaten, die künftige Entdeckungen verhindern wollen.

Insbesondere staatliche Akteure haben ein großes Interesse, die Funktionsweise der Antivirenprodukte zu verstehen. Diese »reverse engineeren unsere Produkte ständig«, schreibt der französische Sicherheitsforscher Ivan Kwiatkowski, Senior Security Researcher bei Kaspersky. Sie versuchen also zu verstehen, wie die Software funktioniert und sich selbst vor Entdeckung zu schützen. »Wenn die NSA noch nicht jede einzelne Anweisung unseres Antivirenprogramms überprüft hat, dann macht jemand einfach seine verdammte Arbeit nicht« – wenn es versteckte Funktionen wie Hintertüren gäbe, wüsste der US-Geheimdienst davon. Und natürlich würde dieser das nutzen, um Kaspersky zu diskreditieren. Nachdem selbst Akteure wie die NSA bisher keine Hintertüren enttarnt hätten, sei es »an der Zeit anzunehmen, dass diese Hintertüren nicht existieren.«

Wie berechtigt ist die BSI-Warnung?

Ist die Warnung des BSI also übertrieben? Manch anderes

Sicherheitsunternehmen – beispielsweise aus den USA – spielt offenbar durchaus mit dem Gedanken, die Hackingtools des eigenen Staates und dessen Spionageoperationen nicht zu veröffentlichen. Das heißt, die Sicherheitsbranche bliebe quasi »blind« gegenüber entsprechenden Viren und Trojanern. Bei Kaspersky ist das möglicherweise anders – das geht zumindest aus zahlreichen Gesprächen vor, die die Autorin mit Sicherheitsforschenden des Unternehmens geführt hat. Belegen lässt es sich freilich nicht zweifelsfrei.

»Damals habe ich mich gefragt: Was ist, wenn wir legitime staatliche Operationen zerstören?«

(Costin Raiu, Direktor des Global Research and Analysis Team)

Der Direktor des Global Research and Analysis Team (GReAT) von Kaspersky, Costin Raiu, sagte bei einem Interview gegenüber der Autorin über den Umgang mit staatlichen Operationen bereits vor den aktuellen Vorfällen, dass er selbst lange über diese Frage nachgedacht und sie auch mit seinem Unternehmen diskutiert habe – unter anderem während der Spionageangriffe verschiedener Staaten, die ab 2011 auf den Computerwurm Stuxnet folgten, hinter dem sich ein Angriff der USA und Israels auf das iranische Atomprogramm verbarg. »Damals habe ich mich gefragt: Was ist, wenn wir legitime staatliche Operationen zerstören? Wenn beispielsweise Terroristen gejagt werden?« Er habe zu dem Zeitpunkt mit seinem Unternehmen darüber diskutiert und schließlich von oberster Stelle die Aussage

bekommen, dass es im Sinne von Kaspersky sei, jegliche Schadsoftware zu enttarnen. Auch die von Staaten – egal von welchen.

Die Frage stellt sich bis heute: Wie gehen Sicherheitsforschende damit um, wenn sie auf staatliche Aktivitäten des eigenen Staats stoßen? Im Frühjahr 2021 wurde diese Diskussion erneut geführt, nachdem ein Google-Sicherheitsteam im Herbst 2020 eine ausgefeilte Spionageattacke entdeckt und öffentlich gemacht hatte. Offenbar gab es intern hitzige interne Diskussionen vor der Veröffentlichung, als herauskam, dass die Spionageoperation die einer verbündeten Nation der USA war. Um welche Nation es sich handelt, verriet Google nicht.

Staatliche Angriffe bleiben oft geheim

In der Diskussion wurde aber klar, dass manche Sicherheitsunternehmen die Operationen ihres eigenen Staats nicht veröffentlichen. Andere warnen die eigenen und verbündete Staatshacker, wenn sie deren Angriff entdeckt haben und geben ihnen eine gewisse Zeit, aufzuräumen, bevor sie die entdeckte Schwachstelle veröffentlichen. Wiederum andere haben eine Abmachung, die Angriffe nicht öffentlich zu machen, wenn sowohl das Sicherheitsteam als auch die Angreifer als »befreundet« gelten – zum Beispiel, wenn ihre Länder Mitglieder der »Five Eyes«-Geheimdienstallianz sind.

Diese Allianz setzt sich aus den Vereinigten Staaten, dem Vereinigten Königreich, Kanada, Australien und Neuseeland zusammen. Für einige Mitglieder der Sicherheitsteams von Google sind solche Entscheidungen sicher nicht leicht, denn sie haben zuvor für westliche Geheimdienste gearbeitet. In dieser Rolle haben manche von ihnen für diese Regierungen digitale Angriffe entwickelt und ausgeführt. Sie haben die Seiten

gewechselt – oder auch nicht? Was ist, wenn solche Interessen auf einmal miteinander kollidieren?

Google hat in diesem Fall darauf verzichtet, den Angreifer öffentlich zu identifizieren und auch einige technische Details in der Veröffentlichung weggelassen. Solche Schwachstellen generell zu veröffentlichen, sei aber wichtig, betonte eine Sprecherin gegenüber »Technology Review«: Das erhöhe die Sicherheit aller.

Kaspersky-Forscher Raiu sieht das ähnlich: »Jede Malware muss entdeckt und gestoppt werden.« Er möchte nicht über sinnvolle Schadsoftware diskutieren, denn die gibt es aus seiner Sicht nicht. Letztlich sei es Sache jener Geheimdienste, die »legitime Malware« machen – falls es diese überhaupt gebe –, besser zu werden. »Wenn du geschnappt wirst, dann bist du zu schlecht gewesen. Das ist nicht unser Problem.« Schließlich endet alles andere in einem gesellschaftlichen Problem: »Wir müssen alle Malware stoppen, denn sie kann auch von anderen genutzt werden und großen Schaden anrichten.«

In der vergangenen Woche haben führende Kaspersky-Forscher um Raiu zudem in einem Webinar ausführlich über die aktuellen Cyberangriffe auf ukrainische Infrastrukturen gewarnt und sich auch nicht gescheut, diese in Verbindung zu bringen mit bekannten Hackergruppen des russischen Geheimdienstes.

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

(Eugene Kaspersky)

Es drängt sich der Eindruck auf, dass Kaspersky-Forscher mit ihrem eigenen Staat gnadenloser umgehen als Sicherheitsforscher anderer Länder mit den Hackingwerkzeugen ihrer jeweiligen Geheimdienste. Allerdings geht der russische Staat offenbar auch gnadenloser mit seinen Gegnern um als manch andere Staaten. Und das ist der Haken an der aktuellen Debatte, der sich von außen schwer beurteilen lässt: Schafft Kaspersky es in seinem russischen Hauptsitz, lediglich loyale Mitarbeitende zu beschäftigen oder zumindest die Aktivitäten systemtreuer Mitarbeiter so weit im Auge zu behalten, dass sie keinen Schaden anrichten können für internationale Kunden?

Auf neutralem Boden

Im November 2018 hat Kaspersky ein Datencenter in der Schweiz eröffnet und damit der Diskussion ein Stück weit nachgegeben: Seither stehen die Server, auf denen Kaspersky die europäischen Kundenanfragen verarbeitet, in Zürich-Glattbrugg. Kaspersky will damit Neutralität demonstrieren. Der Öffentlichkeit zeigen, dass die 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. Natürlich können vermutlich auch die russischen Kaspersky-

Mitarbeiter auf die Server in der Schweiz zugreifen: Viren kennen keine Grenzen, und das muss allein deshalb ebenso für Virenjäger gelten.

Wäre es nicht eine Lösung, ganz in die Schweiz umzuziehen und Moskau endgültig den Rücken zu kehren? Darauf gab Eugene Kaspersky in der Pressekonferenz, in der er seine »Transparenzinitiative« vorstellte, eine verblüffend einfache Antwort: Würde er gern, aber das ist zu teuer. »Für das Gehalt, das ein Softwareentwickler in der Schweiz verlangt, können Sie in Russland fünf Entwickler anstellen.«

Aber kann es sich das Unternehmen leisten, in Russland zu bleiben? Lässt es sich von dort aus sicher betreiben, wenn die Mitarbeitenden und ihre Familien direkt dem Druck russischer Behörden ausgeliefert sind? Denn das BSI betont, dass ein russischer IT-Hersteller auch gegen seinen Willen gezwungen werden könne, Zielsysteme anzugreifen, »oder selbst als Opfer einer Cyberoperation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden« kann.

Ivan Kwiatkowski berichtet in seinem Blogpost von internen Maßnahmen, die davor schützen sollen, dass Insider oder eingeschleuste Spione Schaden anrichten können. Kaspersky ist durchaus zuzutrauen, vieles mitzubekommen von dem, was in den internen Netzen abläuft. So stellte das Unternehmen 2017 fest, dass sich Spione – mutmaßlich des israelischen Geheimdienstes – in ihrem System umschauten, offenbar so gut getarnt, dass sich Sicherheitsfachleute fragten, wie Kaspersky diese überhaupt entdeckt hatte.

Wie gut diese internen Maßnahmen sind und ob es überhaupt möglich ist, die Kunden hundertprozentig davor zu schützen,

dass der russische Geheimdienst in irgendeiner Form doch in die Systeme eindringt, lässt sich freilich von außen schwer einschätzen. Die Energie der russischen Staatshacker, wenn es darum geht, kritische Infrastrukturen digital anzugreifen, sollte jedenfalls nicht unterschätzt werden – das zeigt die Geschichte.

Eva Wolfangel

Die Autorin ist Wissenschaftsjournalistin in Stuttgart und schreibt schwerpunktmäßig über Technologiethemen.