Die skandalösen Hintergründe zum US-Verbot der Antivirensoftware von Kaspersky

„Die USA ‚explodiert' nachdem ein russisches Unternehmen eine "CIA-Hintertüre" geschlossen hat, die in alle Microsoft Software einprogrammiert wurde"

In praktisch allen deutschsprachigen US-hörigen Mainstream-Medien konnte man am **13. September** etwa folgende Schlagzeilen lesen (hier aus NZZ online)

„USA verbieten Kaspersky-Software aus Angst vor dem russischen Geheimdienst"

„Der russische Software-Konzern Kaspersky steht im Verdacht, mit den Behörden in Moskau zusammen zu arbeiten. Hat der russische Geheimdienst Einfluss auf die Sicherheitssoftware?

Das US-Ministerium für Innere Sicherheit teilte am Mittwoch mit, es sei besorgt über mögliche Verbindungen zwischen Firmenvertretern und russischen Geheimdiensten. Es bestehe das Risiko, dass die russische Regierung den Zugang über Kaspersky-Produkte ausnutzen könne, um Informationssysteme der amerikanischen Behörden zu kompromittieren, hiess es in einer Mitteilung.

Die Sicherheitssoftware von Kaspersky gewähre umfassenden Zugang auf Dateien und Administrationsrechte von Computern, auf denen sie installiert sei, erklärte das amerikanische Ministerium. Die Behörden hätten 60 Tage Zeit, um Pläne zu entwickeln, wie die Benutzung der Programme gestoppt werden könne, und 90 Tage, um diese umzusetzen."

Immerhin wird auch ein Sprecher von Kaspersky Lab zitiert, der betont, dass die amerikanischen Behörden keine Beweise vorgelegt hätten, und:

«Sämtliche Anschuldigungen basieren auf Lügen. Das Unternehmen pflegt keinerlei politische Beziehungen zu irgendeiner Regierung, einschliesslich der russischen», sagte der namentlich nicht genannte Sprecher. Kaspersky arbeite seit 20 Jahren in der Sicherheitsbranche und halte die höchsten Standards ein. Zudem betonte er, dass Kaspersky die Daten seiner Nutzer schütze.

Und dies sind offenbar die bedenklichen Hintergründe dieses Verbots, so wie sie, gemäss Sorcha Faal, in einem russischen Bericht enthalten sind:

Von Sorcha Faal, „wie es an die westlichen Abonnenten am **11. September** berichtet wurde", auf Whatdoesitmean.com; übersetzt von Taygeta

Ein beunruhigender Bericht, der heute im Kreml vom Ministerium für Industrie und Handel (MINPROMTORG) herausgegeben wurde, besagt, dass die Vereinigten Staaten in Rage geraten seien und mit "Wut und Vergeltung" reagieren würden gegenüber dem russisch-britischen Unternehmen ***Kaspersky Lab***, nachdem die Experten dieses Cybersicherheitsunternehmens eine "Hintertür" gefunden hätten (das die gebräuchlichen

Sicherheits-Mechanismen der Computer umgeht), welche durch die Central Intelligence Agency (CIA) in alle Microsoft-Software-Produkte eingebracht wurde – und nachdem dies entdeckt worden war die gleichen Kaspersky Lab-Experten einen “Schutz-Patch” (der Computer-Sicherheits-Schwachstellen behebt) herausgegeben hätten, der diese CIA “Hintertür” so “schliesst”, dass sie nicht mehr geöffnet werden kann. [Anmerkung von Sorcha Faal zum in Englisch erschienenen Bericht: “Einige Wörter und / oder Phrasen, die in Zitaten in diesem Bericht erscheinen, sind englischsprachige Approximationen von russischen Wörtern / Phrasen ohne genaues Gegenstück.”]

Nach diesem Bericht ist Kaspersky Lab eines der weltweit grössten privaten Cybersicherheitsunternehmen, das in 200 Ländern und Territorien tätig ist und 37 Büros in 32 Ländern hat. Das Unternehmen wurde 1997 durch den vom russischen Militärgeheimdienst geschulten Computerspezialisten Eugene Kaspersky und seiner Frau Natalya gegründet. Sie waren die ersten in der Welt, die Software entwickelten, um Computerviren zu entdecken, zu überwachen und sie in isolierte Quarantäne zu stellen.

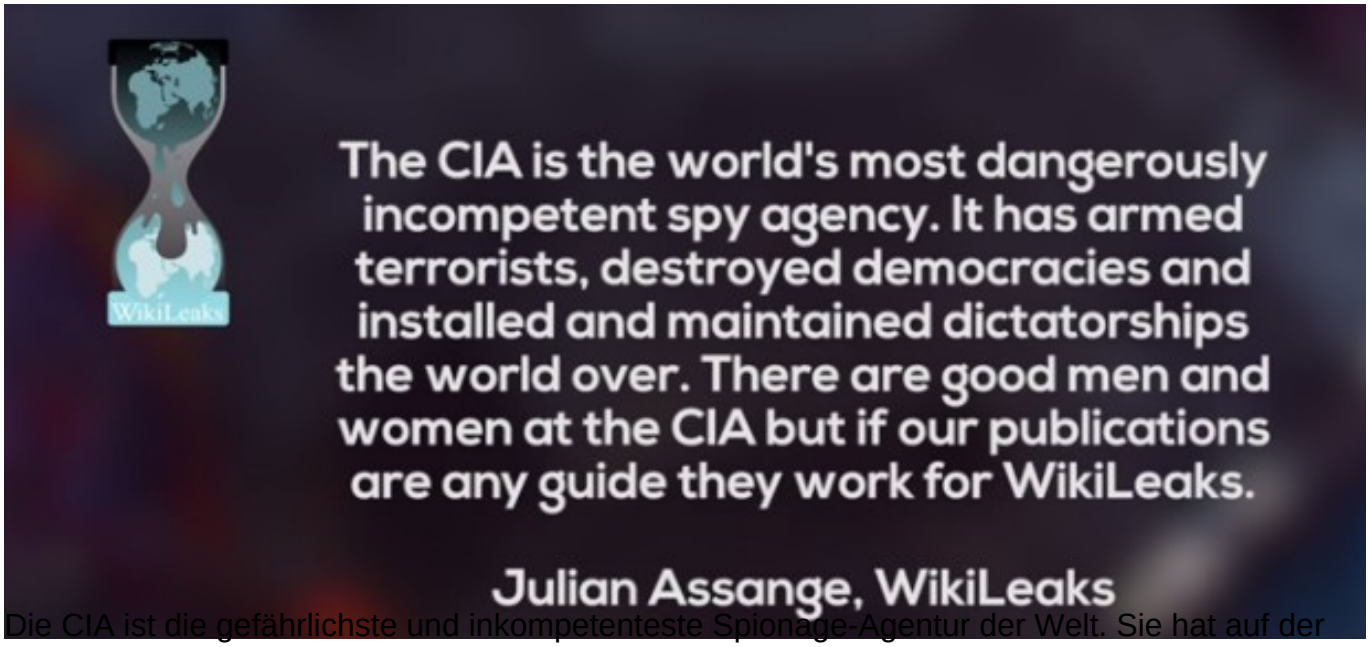
Die Berichte über die Erfolge von Kaspersky Labs bei der Bekämpfung von Computerviren sind zu zahlreich, um aufgezählt zu werden, fährt dieser Bericht weiter, und die globalen Errungenschaften dieses Unternehmens wurden sehr gefeiert – ganz besonders ihre Erfolge bei der Vereitelung von Eingriffen der US-Geheimdienste, die glauben ein Recht auf Spionage zu haben, nicht nur auf jedem einzelnen Amerikaner zielend, sondern auch auf der ganzen Welt. So schrieb etwa The Economist im Jahr 2015:

“Kaspersky Lab hat wiederholt Skeptiker beeindruckt, indem es echte und ernste Cyber-Sicherheitsprobleme aufdeckte. Im Jahr 2010 hat die Firma zum Beispiel dazu beigetragen, dass Stuxnet enttarnt wurde, ein Computer-Wurm, der entworfen wurde, um das

iranische Atomprogramm zu sabotieren.
Am 16. Februar konnte offenbar Kaspersky dieses Kunststück wiederholen, nicht einmal, sondern zweimal.
Zuerst veröffentlichten sie einen Bericht, der beschrieb, wie eine Bande, Carbanak genannt, die Computersysteme von Banken auf der ganzen Welt gehackt hatte. Er besagte, dass die Bande mehrere hundert Millionen Dollar gestohlen hatte, indem sie Geld auf gefälschte Konten leitete und Geldautomaten ihren Inhalt ausspucken liess.
Am selben Tag sagte die Firma, dass sie die "Equation Group" entdeckt hatte, die anscheinend ein Teil der NSA ist und die in der Lage war, Spionagessoftware in Computer einzubetten, um dem Spionage-Geheimdienst die volle Kontrolle über die Computer zu geben, dies auch nachdem die Festplatte gelöscht wurde und das Betriebssystem neu installiert worden ist."

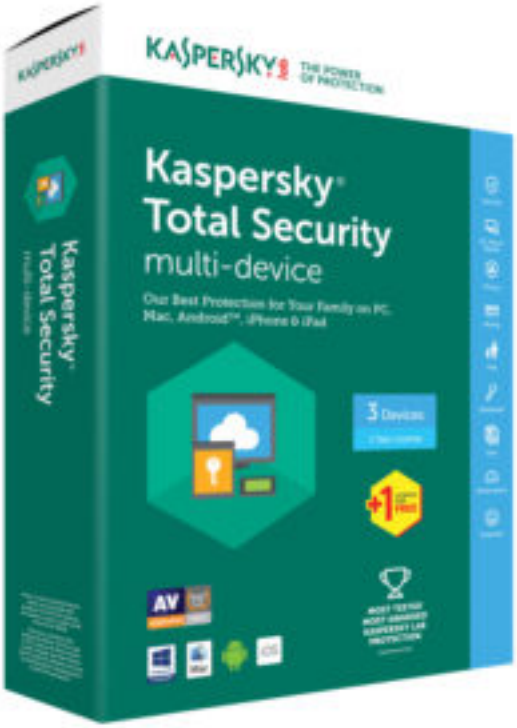
Am 12. Mai dieses Jahres, so weist dieser Bericht auf weitere Details hin, hat die internationale Whistle Blowing Organisation ***WikiLeaks*** die neueste Tranche in ihrer Vault7-Serie veröffentlicht (Warnung: Es ist illegal für Personen mit US-Sicherheitsfreigaben auf diesen Link zu klicken). Darin werden detailliert zwei CIA Hacking-Tools angegeben, genannt *'AfterMidnight'* und *'Assassin'*, die auf die Microsoft Windows-Plattform abzielen. Diese Spionage-Software erlaubt es der CIA, einen umfassenden Zugriff auf jedermanns Computer oder Handy zu ermöglichen. [Im Rahmen der Vault7 – Veröffentlichungen von WikiLeaks wurden viele weitere ***Spionage- und Malware-Tools*** enttarnt, die von der CIA eingesetzt werden. Man kann sich im Netz darüber selbständig kundig machen. Man muss dazu nur die ***Namen dieser Programme*** in Suchmaschinen eingeben: *Angelfire, Grasshopper, Achilles, Aeris, SeaPea, Highrise, Pandemic, Athena, Scribbles, Marble Framework, Dark Matter* … und wie sie alle heissen; vgl. z.B. hier]

Gemäss dem Bericht haben die Kaspersky Lab-Experten, die diese (von WikiLeaks veröffentlichten) CIA-Hacking-Tools untersuchten, eine "Hintertür" in der Form eines Programms mit dem Namen "PsSetLoadImageNotifyRoutin" entdeckt, das in die gesamte Microsoft-Software eingebettet ist, und welche die Antivirensoftware sadistisch daran hindert, Computervirus-Malware zu finden – und dass Microsoft sich weigerte, einen Sicherheits-Patch dazu zu veröffentlichen, mit der verblüffenden Feststellung: „Unsere Ingenieure haben die Informationen überprüft und festgestellt, dass dies keine Sicherheitsbedrohung darstellt. Wir planen deshalb nicht, es mit einem Sicherheitsupdate anzugehen."



Die CIA ist die gefährlichste und inkompetenteste Spionage-Agentur der Welt. Sie hat auf der ganzen Welt Terroristen ausgerüstet, Demokratien zerstört und Diktaturen eingesetzt und unterhalten. Es gibt gute Frauen und Männer bei der CIA, aber wenn unsere Publikationen eine Hilfe sind, dann arbeiten sie für WikiLeaks.

Der Bericht hält weiter fest, dass nachdem Microsoft es nicht schaffte, ihre Software vor dieser “CIA-Hintertür” zu schützen, Kaspersky Lab ihre eigene “Fix”-Software schuf, welche sie in ihr eigenes globales Anti-Virus-Software-Produkt namens Kaspersky Total Security einbaute, und dies bereits im vergangenen Juni.



Unmittelbar nachdem Kaspersky Lab diesen “Fix” veröffentlicht hatte, um Menschen und ihre Microsoft-Software und Computer vor dieser “CIA-Hintertür” zu schützen, begann das FBI mit nächtlichen Angriffen gegen die Mitarbeiter dieses Unternehmens in den Vereinigten Staaten und ging über zu einer bösartigen

Kampagne, in der private Unternehmen in Amerika aufgefordert wurden, das Kaspersky Total Security Anti-Virus-Programm nicht mehr zu nutzen, weil es eine “unannehmbare Bedrohung für die nationale Sicherheit” darstelle – ohne irgendjemandem in den USA einen Beweis für diese unverschämte Behauptung zu unterbreiten.

Als Reaktion auf diesen Angriff gegen seine Firma bot Eugene Kaspersky öffentlich an, den USA den Quellcode zu seinem Kaspersky Total Security Anti-Virus Programm zur Verfügung zu stellen, um zu beweisen, dass es sich nicht um ein Trojanisches Pferd für russische Spione handelt – mit der zusätzlichen Feststellung, dass er auch bereit sei, vor dem Kongress als Zeuge aufzutreten, und “alles” zu zeigen, um zu beweisen, dass seine Firma offen und lupenrein ist.

Anstatt dieses Angebot von Kaspersky zu akzeptieren, und wieder ohne irgendwelche Beweise zu liefern, begann Senator Jeanne Shaheen von der Demokratischen Partei bei der Bundes-Regierung für ein USA-weites Verbot der Anti-Virus-Sicherheitssoftware von Kaspersky Lab zu pushen – und Amerikas grösster Elektronik-Einzelhändler, *Best Buy*, erklärte, dass es alle Kaspersky Lab Anti-Virus-Produkte sofort aus seinen Laden-Regalen entfernen werde. Überdies bot *Best Buy* an, dass ihre Support-Organisation *Geek Squad*, allen Kunden behilflich sein werde, um das Programm aus deren Computern zu entfernen, verschwieg dabei allerdings, dass ihre Geek Squad Tech-Arbeiter auch von der FBI angestellt sind, um heimlich auf den Computern der Kunden nach Kinderpornographie zu suchen.

Der “rote Hering” (eine Bezeichnung für etwas, das die Aufmerksamkeit von einer viel wichtigeren Frage ablenken soll), der von den USA gegen Kaspersky Lab verwendet wird, erklärt dieser Bericht, ist seine vermeintliche “Verbindung” zur russischen Regierung und den russischen Geheimdiensten [Siehe den oben zitierten Artikel der NZZ]. Dies ist eine

erstaunliche und unverschämte Anschuldigung von einer Nation, deren CIA alle Microsoft Windows-PCs auf der ganzen Welt mit verborgener Software in Spionage-Werkzeuge verwandelt hat und nach Wunsch über diese “Hintertüren” aktivieren kann, ebenso über Windows Updates. Mit ihren Patriot Act-Gesetzen geben die USA ihren Spionage-Agenturen die unbegrenzte Macht, um alle Computer, E-Mails, Telefonate und was immer man will auf der ganzen Welt auszuspionieren.

Dieser Bericht schliesst mit der Feststellung, dass diese “Erkenntnisse und Ermittlungen” die Grundlage bildeten für die Anordnung von Präsident Putin, dass Russland sich von ausländischer Software unabhängig machen soll, im Interesse der Sicherheit – und allen russischen Leuten empfahl: “Sie sollten keine IBM Produkte anbieten oder ausländische Software. Wir können sie nicht nehmen, weil sie zu viele Risiken bergen.”

Vgl. dazu die Notiz von rt vom 9. September: Russland muss aus Sicherheitsgründen von ausländischen Software-Produkten abrücken

Hast du dich je gewundert, warum diese Tech-Firmen so reich wurden?