In einem Memorandum an Präsident Trump zitiert eine Gruppe ehemaliger Geheimdienstbeamter und NSA-Experten neue kriminaltechnische Untersuchungen, die die grundlegende Einschätzung des „Intelligence Community Assessment“ vom 6. Januar 2017 in Zweifel ziehen, dass Russland im vergangenen Jahr Emails der Demokraten „gehackt“ hat. Aus dem Englischen von **Josefa Zimmermann**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

http://www.nachdenkseiten.de/upload/podcast/170802_Geheimdienstveteranen_bezweifeln_Beweise_fuer_russischen_Hackerangriff_NDS.mp3

Podcast: Play in new window | Download

Memorandum an: Den Präsidenten
Von: Veteran Intelligence Professionals for Sanity (VIPS)
Betreff: War der „russische Hackerangriff“ in Inside Job?

Zusammenfassung

Kriminaltechnische Untersuchungen über den “russischen Hackerangriff” auf die Computer des Nationalkomitees der Demokraten (DNC) im vergangenen Jahr zeigen, dass am 5. Juli 2016 Daten von einer Person mit direktem Zugang zu den DNC-Computern „geleakt“ und nicht „gehackt“ wurden, um die Tat danach Russland in die Schuhe zu schieben.

Nach der Untersuchung von Metadaten über das Eindringen von “Guccifer 2.0” in den DNC-Server am 5. Juli 2016 stellten unabhängige Cyber-Ermittler fest, dass ein Insider die DNC-Daten auf ein externes Speichermedium kopierte und “verräterische Zeichen” hinterließ, um den Verdacht auf Russland zu lenken.

Der Schlüssel zu den Ergebnissen der unabhängigen kriminaltechnischen Untersuchungen ist die Tatsache, dass die DNC-Daten mit einer Geschwindigkeit auf das Speichermedium kopiert wurden, die bei einem Hackerangriff von außen nicht möglich gewesen wäre. Ebenso wichtig ist das Ergebnis, dass die Daten an der Ostküste der USA kopiert und bearbeitet wurden. Die Mainstream-Medien ignorierten die Ergebnisse dieser unabhängigen

Untersuchungen bis heute. [siehe hier und hier].

Skip Folden, unabhängiger Analyst und IBM-IT-Manager im Ruhestand, der die kriminaltechnischen Befunde überprüfte, ist Mitverfasser dieses Memorandums. Er schrieb einen detaillierten Bericht mit dem Titel “Cyber-kriminalistische Untersuchung des ‘russischen Hackerangriffs’ und das fehlende Dementi der Geheimdienste”, und schickte ihn an die Büros des Sonderberaters und des Generalstaatsanwaltes. William Binney, VIPS-Mitglied und ehemaliger Technischer Direktor bei der National Security Agency (NSA) sowie andere ehemalige NSA-Mitarbeiter bei VIPS bescheinigten die Professionalität der unabhängigen kriminaltechnischen Befunde.

Diese neuen kriminaltechnischen Studien füllen eine wichtige Lücke. Es bleibt ein Rätsel, warum das FBI es versäumt hat, das Originalmaterial von “Guccifer 2.0” einer unabhängigen kriminaltechnischen Überprüfung zu unterziehen. Ebenso rätselhaft bleibt, warum es keinen Hinweis darauf gibt, dass die “handverlesenen Analysten” von FBI, CIA und NSA als Verfasser des „Intelligence Community Assessment“ vom 6. Januar 2017 die kriminaltechnischen Ergebnisse nicht berücksichtigten.

ANMERKUNG: Aufgrund der zahlreichen Klagen über Hackerangriffe möchten wir deutlich machen, dass der Hauptfokus dieses Memorandums auf dem angeblichen Guccifer-2.0-Angriff vom 5. Juli 2016 auf den DNC-Server liegt. In früheren VIPS-Memoranden wiesen wir auf das Fehlen von Beweisen für eine Verbindung zwischen dem angeblichen Guccifer-2.0-Angriff und WikiLeaks hin und baten Präsident Obama, spezifische Beweise dafür offenzulegen, dass WikiLeaks die DNC-Daten von den Russen erhalten hatte. [siehe hier und hier].

Als er diesen Punkt bei seiner letzten Pressekonferenz am 18. Januar ansprach, bezeichnete er “die Erkenntnisse der Geheimdienste” als “nicht schlüssig”, obwohl das „Intelligence Community Assessment“ vom 6. Januar sich ziemlich sicher war, dass der russische Geheimdienst “Material, das vom DNC stammte, … an WikiLeaks weitergegeben hat“.

Obamas Eingeständnis war nicht überraschend. Uns ist schon lange klar, dass der Grund für das Fehlen schlüssiger Beweise der US-Regierung für die Weitergabe der Hackerdaten an WikiLeaks durch Russland darin liegt, dass es diese Weitergabe nicht gab. Basierend auf der einzigartigen gemeinschaftlichen technischen Expertise unserer Ex-Kollegen von der NSA sind wir seit einem Jahr der Überzeugung, dass die DNC-Daten durch eine Kopie oder ein Datenleck von einem DNC-Insider an WikiLeaks übermittelt wurden, wobei der Übermittler der Daten und derjenige, der sie am 5. Juli 2016 kopiert hat, mit großer Sicherheit nicht ein- und dieselbe Person waren.

Aus den verfügbaren Informationen schließen wir, dass die Copy/Leak-Aktion durch DNC-Insider zu zwei verschiedenen Zeitpunkten von zwei verschiedenen Personen durchgeführt und zu zwei deutlich unterscheidbaren Zwecken verwendet wurde:

1. ein Datenübermittlung durch Insider an WikiLeaks im Vorfeld der Ankündigung von Julian Assange am 12. Juni 2016, dass er DNC-Dokumente besitzt und plant, sie zu veröffentlichen, was am 22. Juli 2016 geschah – vermutlich mit dem Ziel, der Clinton-Kandidatur zu schaden – und
2. eine separates „Leak“ am 5. Juli 2016, um im Vorgriff auf spätere Veröffentlichungen von WikiLeaks zu „beweisen“, dass ein „russischer Hackerangriff“ dahintersteckte.

Herr Präsident,

dies ist unser erstes VIPS-Memorandum an Sie, aber wir haben langjährige Erfahrung darin, die US-Präsidenten zu informieren, wenn wir den Eindruck haben, dass unsere ehemaligen Geheimdienstkollegen mit ihrer Einschätzung falsch liegen und warum. Zum Beispiel warnte unser erstes Memorandum, ein aktueller Kommentar an Präsident George W. Bush über die UN-Rede von Colin Powell am 5. Februar 2003, dass die “unbeabsichtigten Konsequenzen wahrscheinlich katastrophal sein würden”, falls die USA den Irak angreifen und den Krieg mit Geheimdienstinformationen rechtfertigen sollten, die wir ehemaligen Geheimdienstoffiziere ohne Weiteres als betrügerisch und von einer Kriegsagenda getrieben erkennen konnten.

Das “Intelligence Community Assessment” vom 6. Januar 2017, erstellt von „handverlesenen“ Analysten von CIA, FBI und NSA, scheint uns in die gleiche, von einer Agenda geleitete Kategorie zu passen. Es stützt sich weitestgehend auf die unbewiesene Vermutung, dass eine dunkle Kreatur mit dem Decknamen „Guccifer 2.0“ im Auftrag des russischen Geheimdienstes einen Hackerangriff gegen den DNC ausführte und DNC-Emails an WikiLeaks weitergab.

Die oben erwähnten jüngsten kriminaltechnischen Befunde haben dieser Einschätzung einige Kratzer zugefügt und ernsthafte Zweifel an den Grundlagen der außerordentlich erfolgreichen Kampagne gesät, die die russische Regierung für den Hackerangriff verantwortlich machte. Von den Experten und Politikern, die die These von der russischen “Einmischung” in die US-Wahl verbreiteten, konnte man nichts anderes erwarten als den Versuch, die kriminaltechnischen Erkenntnisse jedes Mal in Zweifel zu ziehen, wenn sie das Thema in den Mainstream-Medien aufbauschten. Aber die Grundlagen der Physik sind weiterhin gültig und die technischen Grenzen des heutigen Internets sind bekannt. Wir sind bereit, ihre Leistungen in Frage zu stellen.

Vielleicht sollten Sie den CIA-Direktor Mike Pompeo fragen, was er über diese Angelegenheit weiß. Aufgrund unserer eigenen jahrelangen Geheimdiensterfahrung vermuten wir, dass womöglich weder der frühere CIA-Direktor John Brennan, noch seine Cyberkrieger gegenüber ihrem neuen Direktor ganz ehrlich waren bezüglich dieses Fehlschlages.

Kopiert, nicht gehackt

Wie oben gezeigt, fokussierte sich die kürzlich abgeschlossene kriminaltechnische Untersuchung auf Daten, die von einem geheimnisvollen Wesen namens Guccifer 2.0 kopiert und nicht gehackt wurden. Die Kriminalisten zeigten, dass ein verzweifelter Versuch unternommen worden war, die Veröffentlichung der peinlichen DNC-Emails drei Tage vor dem Konvent der Demokraten im letzten Juli den Russen in die Schuhe zu schieben. Da der Inhalt der DNC-Emails nach Begünstigung von Clinton roch, war es notwendig, in ihrem Wahlkampf die Aufmerksamkeit vom Inhalt weg auf die Herkunft zu lenken – im Sinne von „Wer hat diese Emails gehackt?“ Die Mainstream-Medien unterstützten die Kampagne begeistert und bereitwillig und sie ist immer noch nicht zu Ende.

„Die Russen“ waren die idealen Sündenböcke. Und nachdem WikiLeaks-Chef Julian Assange am 12. Juni 2016 angekündigt hatte, “Wir besitzen Emails, die Hillary Clinton betreffen und die wir zu einem späteren Zeitpunkt veröffentlichen werden“, hatte ihr Wahlkampfteam vor dem Konvent noch mehr als einen Monat Zeit, um seine eigenen “kriminaltechnischen Fakten” zu setzen und die Medienmühle in Gang zu bringen, die die Russen der „Einmischung“ beschuldigte. Frau Clintons PR-Chefin Jennifer Palmieri erzählte, wie sie mit einem Golf-Caddy Runden auf dem Parteikonvent drehte. Sie schrieb, dass es „ihre Mission war, das Interesse der Presse auf etwas zu lenken, das für uns selbst schwer zu vermitteln war”, die Sichtweise, dass Russland nicht nur Emails gehackt und dem DNC gestohlen hatte, sondern auch noch aus dem Grund, Donald Trump zu unterstützen und Hillary Clinton zu schaden.

Unabhängige Cyber-Ermittler haben nun die kriminaltechnische Arbeit dort vervollständigt, wo die Annahmen der Geheimdienstbeamten Lücken gelassen hatten. Seltsamer Weise ergingen sich die „handverlesenen“ Beamten nur in dieser oder jener Vermutung. Im Gegensatz dazu gruben die Ermittler tief und förderten reale Beweise zutage, bestehend aus Metadaten, die sie in den Akten über den angeblichen russischen Hackerangriff fanden.

Sie fanden heraus, dass es sich bei der Guccifer-2.0-Aktion nicht um einen Hackerangriff handelte, weder um einen russischen noch um irgendeinen anderen. Vielmehr stammten die Daten von einer Kopie auf einem externen Speichermedium, beispielsweise einem USB-

Stick, den ein Insider erstellt hatte. Die Daten wurden „geleakt“, nachdem sie durch Kopieren und Einfügen so bearbeitet worden waren, dass der Verdacht auf Russland fiel. Wir haben keine Ahnung, wer dieser dunkle Guccifer 2.0 ist. Vielleicht fragen Sie einmal beim FBI nach.

Der zeitliche Ablauf

12. Juni 2016: Assange kündigt an, dass WikiLeaks Emails veröffentlichen wird, „die Clinton betreffen“.

15. Juni 2016: DNC-Vertragspartner Crowdstrike (von zweifelhaftem professionellen Ruf und mit vielen Interessenskonflikten) gibt bekannt, dass Malware auf dem DNC-Server gefunden wurde und behauptet, es gäbe Beweise für die Urheberschaft der Russen.

15. Juni 2016: „Guccifer-2.0“ bestätigt am selben Tag die Stellungnahme des DNC und bekennt sich zu dem Hackerangriff. Er behauptet, der WikiLeaks-Informant zu sein und postet ein Dokument, auf dem die Kriminalisten später künstlich eingefügte „russische Fingerabdrücke“ finden.

Wir glauben nicht, dass das Timing am 12. und 15. purer Zufall war. Vielmehr zeigt es den Beginn einer Präventivmaßnahme, die Russland im Vorfeld mit etwas in Verbindung bringen sollte, das WikiLeaks möglicherweise später veröffentlichen würde, um zu beweisen, dass Russland der Übeltäter ist.

Das Schlüsselereignis

5. Juli 2016: Am frühen Abend, als es an der Ostküste noch Tag ist, arbeitet jemand in der Ostküsten-Zeitzone an einem Computer, der direkt mit dem DNC-Server oder mit dem Local Area Network verbunden ist. Die Person kopierte 1.976 MB Daten innerhalb von 87 Sekunden auf einen externen Datenspeicher. Das ist um ein Vielfaches schneller, als es bei einem Hackerangriff möglich wäre.

Daher sieht es danach aus, dass das angebliche Hacken des DNC durch Guccifer 2.0 (der selbsternannte WikiLeaks-Informant) weder von Russland aus noch von einem Außenstehenden ausgeführt wurde, sondern es wurden DNC-Daten auf ein externes Speichermedium kopiert. Darüber hinaus stellten die Kriminaltechniker durch Untersuchung der Metadaten fest, dass danach durch das künstliche Einfügen einer russischen Vorlage mit „Cut and Paste“ ein russischer Hackerangriff simuliert werden sollte. Dies alles geschah im Bereich der Ostküsten-Zeitzone.

Vertuschung und Aufdeckung

Herr Präsident, die unten beschriebene Aufdeckung kann damit im Zusammenhang stehen. Sollte das nicht der Fall sein, so glauben wir trotzdem, dass Sie sich dieses allgemeinen Zusammenhangs bewusst sein sollten. Am 7. März 2017 begann WikiLeaks mit der Veröffentlichung einer großen Menge von Originaldokumenten der CIA unter der Bezeichnung “Vault 7“. WikiLeaks bemerkte dazu, dass die Dokumente von einem aktuellen oder ehemaligen CIA-Vertragspartner stammen und dass sie in Umfang und Bedeutung vergleichbar sind mit den Informationen, die Edward Snowden 2013 den Reportern übergab.

Niemand bezweifelte die Echtheit der Originaldokumente von Vault 7, die eine breite Palette von Instrumenten der digitalen Kriegsführung enthielten, die wahrscheinlich mit Hilfe der NSA von der CIA Engineering Development Group entwickelt wurden. Diese Gruppe war Teil der weitverzweigten CIA-Abteilung für digitale Innovation – ein Wachstumszweig, der von John Brennan im Jahr 2015 gegründet worden war.

Dabei handelt es sich um kaum vorstellbare digitale Instrumente, die die Kontrolle über Ihr Auto übernehmen und es zum Beispiel ferngesteuert mit einer Geschwindigkeit von über 100 Meilen pro Stunde rasen lassen können oder Fernspionage durch einen Fernseher ermöglichen. Darüber wurde in der New York Times und in anderen Medien im vergangenen März berichtet. Aber der dritte Teil der Veröffentlichung von Vault 7 am 31. März, der das “Marble-Framework”-Programm öffentlich machte, wurde anscheinend als zu heikel für den Druck angesehen und nicht in der New York Times publiziert.

Wie es aussah, erhielt Ellen Nakashima von der Washington Post „die Meldung nicht rechtzeitig“. Ihr Artikel vom 31. März trug die Aufmerksamkeit erregende (und zutreffende) Überschrift: **“Die neueste WikiLeaks-Veröffentlichung der CIA-Cyber-Tools könnte deren eigene Hacking-Aktivitäten offenlegen“**.

Die WikiLeaks-Veröffentlichung machte deutlich, dass Marble entwickelt wurde für flexible und einfach zu handhabende”Verschleierung” und dass der Marble-Quellcode einen “Entschleierungsmechanismus” enthält, der Textverschleierungen der CIA rückgängig macht.

Noch wichtiger ist, dass die CIA Marble angeblich im Jahr 2016 anwendete. In ihrem Bericht in der Washington Post ließ Nakashima dies zwar aus, wies aber auf einen weiteren wichtigen Punkt bei der WikiLeaks-Veröffentlichung hin: das Verschleierungsinstrument könnte eingesetzt werden, um ein „Doppelspiel bei der kriminaltechnischen Zuordnung“

oder eine False-Flag-Operation durchzuführen, da es Testbeispiele in Chinesisch, Russisch, Koreanisch, Arabisch und Farsi enthielt.

Die Reaktion der CIA war neuralgisch. CIA-Direktor Mike Pompeo schlug zwei Wochen später zu und nannte Assange und seine Mitarbeiter “Dämonen”. “Es ist Zeit, WikiLeaks als das zu bezeichnen, was es wirklich ist, ein nichtstaatlicher feindlicher Geheimdienst, der oft von staatlichen Akteuren wie Russland unterstützt wird”.

Herr Präsident, wir wissen nicht, ob „Marble Framework“ oder ähnliche Instrumente der CIA eine Rolle spielten bei der Kampagne, die Russland für den Hackerangriff auf den DNC verantwortlich machte. Wir wissen auch nicht, wie ehrlich die Mitarbeiter der CIA-Abteilung für Digitale Innovation gegenüber Ihnen und Direktor Pompeo waren. Dies sind Bereiche, die von einer frühzeitigen Überprüfung durch das Weiße Haus profitieren könnten.

Putin und die Technologie

Wir wissen ebenfalls nicht, ob Sie digitale Themen mit Präsident Putin im Detail besprochen haben. In seinem Interview mit Megyn Kelly bei NBC schien er ziemlich offen – vielleicht sogar besonders interessiert – zu sein, auf Probleme einzugehen, die mit der Art digitaler Instumente zu tun haben, die durch Vault 7 öffentlich gemacht wurden, wenn auch nur durch den Hinweis, dass er darüber informiert wurde. Putin wies darauf hin, dass Hackerangriffe durch die heutige Technologie “maskiert und getarnt werden können, sodass niemand den Urheber herausbekommen kann… Und umgekehrt ist es möglich, jede Institution oder Person als vermeintlichen Täter erscheinen zu lassen.”

„Hacker können überall auftauchen”, sagte er. “Vielleicht gibt es Hacker, womöglich in den USA, die sehr professionell Russland die Schuld in die Schuhe schieben können….Können Sie sich ein solches Szenario vorstellen? … Ich kann es.”

Vollständige Offenlegung: In den letzten Jahrzehnten hat das Ethos unseres Berufes als Geheimdienstbeamte in den Augen der Öffentlichkeit sehr gelitten, bis hin zu dem Punkt, dass eine Analyse unabhängig von einer Agenda für nahezu unmöglich erachtet wird. Wir als Mitglieder der VIPS distanzieren uns davon mit allem, was wir sagen und tun: Wir haben keine politische Agenda; Unser alleiniges Ziel ist, die Wahrheit zu verbreiten und, wenn nötig, unsere ehemaligen Geheimdienstkollegen zur Verantwortung zu ziehen.

Wir sprechen und schreiben frei von Bedrohung oder Begünstigung. Folglich ist jede Ähnlichkeit zwischen unseren Äußerungen und denen von Präsidenten, Politikern und Experten rein zufällig. Die Tatsache, dass wir diese Bemerkung für notwendig halten,

spricht Bände über diese hochgradig politisierten Zeiten. Dies ist unser 50. VIPS-Memorandum seit dem Nachmittag, an dem Powell seine Rede vor der UNO hielt. Die Links zu den 49 anderen Memoranden finden Sie hier.

Die Steuerungsgruppe der Veteran Intelligenc Professionals for Sanity

- William Binney, ehemaliger Technischer Direktor für Geopolitische und Militärische Analyse, NSA, Mitbegründer des NSA’s Signals Intelligence Automation Research Center
- Skip Folden, unabhängiger Analyst, ehem. IBM Program Manager for Information Technology US (ehem. Capt., USMC, Iraq & Foreign Service Officer, Afghanistan (Associate VIPS)
- Larry C Johnson, CIA & State Department (i. R.)
- Michael S. Kearns, Air Force Intelligence Officer (i.R.), Master SERE Resistance to Interrogation Instructor
- John Kiriakou, ehem. CIA Counterterrorism Officer, ehem. Senior Investigator, Senate Foreign Relations Committee
- Linda Lewis, WMD preparedness policy analyst, USDA (i. R.)
- Matthew Hoh, fda Lewis, WMD preparedness policy analyst, USDA (i.R.)
- Lisa Ling, TSgt USAF (i. R.) (Associate VIPS)
- Edward Loomis, Jr., ehemaliger NSA Technical Director for the Office of Signals Processing
- David MacMichael, National Intelligence Council (i. R.)
- Ray McGovern, ehem. U.S. Army Infantry/Intelligence officer und CIA Analyst
- Elizabeth Murray, ehem. Deputy National Intelligence Officer for Middle East, CIA
- Coleen Rowley, FBI Special Agent und ehem. Minneapolis Division Legal Counsel (i. R.)

- Cian Westmoreland, ehem. USAF Radio Frequency Transmission Systems Technician und Unmanned Aircraft Systems Whistleblower (Associate VIPS)
- Kirk Wiebe, ehem. Senior Analyst, SIGINT Automation Research Center, NSA
- Sarah G. Wilton, Intelligence Officer, DIA (i. R.); Kommandeurin, US Naval Reserve (i. R.)
- Ann Wright, U.S. Army Reserve Colonel (i.R.) und ehem. US-Diplomatin