Immer wieder geistert die Meldung durch die Gazetten, „russische Hacker“ mit „Verbindungen zu den russischen Diensten“ oder gar „dem Kreml“ hätten dies oder das gehackt und würden über gezielte Informations- und Desinformationskampagnen Einfluss auf Wahlkämpfe nehmen. Die drei großen „Leaks“ im US-Wahlkampf werden dafür gerne als Beleg zitiert und es gilt als ausgemachte Sache, dass „Moskau“ auch in den Bundestagswahlkampf 2017 eingreifen wird. So berichtet es beispielsweise die Frankfurter Sonntagszeitung in ihrer jüngsten Titelstory. Dieses Geraune ist erstaunlich. Bereits ein kleiner Faktencheck zeigt nämlich, dass es in keinem Fall Beweise für eine russische Beteiligung gibt und selbst die Indizien mehr als mager sind. Von **Jens Berger**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

http://www.nachdenkseiten.de/upload/podcast/161207_Russland_Hacker_Faktencheck_NDS.mp3

Podcast: Play in new window | Download

Die DC Leaks, der Hackerangriff auf das DNC und auf Clintons Kampagnenchef John Podesta – drei Fälle von Cyberkriminalität, bei denen wahrscheinlich vertrauliche Daten von Hackern an die Öffentlichkeit gebracht wurden, um Einfluss auf den Wahlkampf zu nehmen. Aber handelt es sich hierbei tatsächlich auch um drei Beispiele dafür, dass Russland Einfluss auf den US-Wahlkampf genommen hat? Immerhin wird dies ja regelmäßig von Politikern und den Medien behauptet.

Um es ganz kurz zu machen: Es gibt keine gesicherte Erkenntnis darüber, wer die verantwortlichen Hacker in diesen drei Fällen waren und auch über die Herkunft der Hacker oder ihren Aufenthaltsort gibt es keine echten Erkenntnisse. Alles was darüber hinaus geht, wie z.B. Verbindungen zu russischen Diensten oder dem Kreml, ist pure Spekulation.

Was ist gesichert?

Als gesichert darf angenommen werden[*], dass im Jahr 2016 zahlreiche US-Politiker samt derem Stab und Beraterteam Ziel von sogenannten Phishing-Attacken waren. Solche Phishing-Attacken kennen freilich nicht nur Politiker; fast jeder E-Mail-Nutzer wird schon mal eine solche Mail bekommen haben. Beliebt sind beispielsweise Mails, die vorgeben, man

müsse sein Kennwort bei PayPal erneuern. Wenn man den Link in der Mail anklickt, kommt man jedoch nicht auf die Seite von PayPal, sondern auf eine – je nach Professionalität der Täter – mehr oder weniger täuschend echte Kopie der PayPal-Seite. Hat man seine Login-Daten auf dieser gefälschten Seite eingegeben, haben die Täter die Daten und können das PayPal-Konto des Opfers leerräumen. Ganz ähnlich funktionierte auch der Trick, mit dem die Hacker an die Mails hochrangiger Politikberater, wie beispielsweise Clintons Kampagnenchef John Podesta gekommen sind.

John Podesta hat – man glaubt es ja kaum – für seine dienstlichen Mails tatsächlich einen kostenlosen Mail-Account beim Internetgiganten Google. Und als Podesta eines Tages eine vermeintliche Warnmeldung von Google bekam, sein Passwort müsse wegen eines Sicherheitsproblems geändert werden, klickte er diese Mail an und gab brav seine Login-Daten ein. Nicht nur Podesta, sondern auch der ehemalige 4-Sterne-General und Außenminister Colin Powell und nahezu das komplette Spitzenpersonal der Demokratischen Partei sowie zahlreicher namhafter Republikaner soll demnach nicht nur Googles kostenloses G-Mail dienstlich nutzen, sondern auch auf derart offensichtliche Phishing-Mails klicken. Soll man das glauben? Mir fällt es zumindest schwer.

Aber nehmen wir mal an, die „offizielle Story“, auf die sich die gesamte Geschichte von den „russischen Hackern“ stützt, ist korrekt. Was ist denn nun „russisch“ an diesem Hack? Darauf haben die involvierten Spezialisten erstaunlicherweise keine direkte Antwort. Um diesen Spin nachvollziehen zu können, muss man schon weiter ausholen.

Sofacy, Guccifer 2.0 und die Wiedergeburt von Felix Edmundowitsch (Dserschinski)

Phishing über gefälschte Mails und Schadsoftware sind ein Milliardengeschäft und das Klischee will es, dass russische Hacker darin besonders aktiv sind. Ob dies überhaupt stimmt, ist offen. Aus kritischen Internetsicherheitskreisen hört man auch immer wieder die Anekdote, nach der die omnipotenten russischen Hacker vielmehr eine PR-Erfindung des russischen IT-Sicherheitsgiganten Kaspersky Lab sind – wenn russische Hacker das größte Problem sind, kann natürlich nur ein russisches IT-Sicherheitsunternehmen die Lösung sein, so die durchschaubare Werbestrategie.

Will man Hacker, Hackerkollektive oder Hackergruppen identifizieren, so ist das in der Regel nur über eine Fallanalyse möglich: Welche Server, welche Strings und Module und welche Schadsoftware wurde genutzt; haben die Hacker Sicherheitslücken genutzt, die zu diesem Zeitpunkt sonst noch niemandem bekannt waren. Eine dieser Hackergruppen, die aufgrund von Fallanalysen immer wieder ermittelt werden kann, ist APT28 bzw. die Sofacy-Gruppe. Dass es diese Gruppe gibt, ist unbestritten. Dass diese Gruppe aus Russen besteht,

ist jedoch pure Spekulation. So entsprächen die Zeitstempel der eingesetzten Software-Module Experten zufolge „den üblichen Arbeitszeiten im europäischen Teil Russlands“. Nun gut, die Türkei ist in derselben Zeitzone und fast ganz Europa ist nur zwei Stunden hinter der Moskauer Zeit. Und da das Klischee es ja so will, dass Hacker nicht unbedingt einen Nine-to-Five-Job haben, erscheint dieses Indiz recht skurril. Gerichtsfest wäre sowas in Deutschland jedenfalls ganz sicher nicht.

Gibt es denn keine besseren Indizien? Besser nicht, aber skurriler alle Male. So sieht es die US-Cybersicherheits-Business-Community beispielsweise als überzeugendes Indiz für eine Beteiligung russischer Sicherheitsdienste an, dass ein Word-Dokument, das vom Hacker Guccifer 2.0, der offenbar für sämtliche Leaks aus dem US-Wahlkampf verantwortlich ist, von einem Benutzer editiert wurde, der das Office-Paket von Microsoft auf den Namen „Феликс Эдмундович“ registrieren lassen hat, also auf Felix Edmundowitsch (Dserschinski), den legendären Gründer der ersten sowjetischen Geheimpolizei, der Tscheka. Das ist nicht nur skurril, sondern schon fast wieder lustig. Offenbar haben die Täter Sinn für Humor.

Irgendwie wirkt die gesamte Geschichte dann auch mehr wie ein nicht besonders guter Witz. Da nutzen die Koryphäen der US-Politik einen kostenlosen E-Mail-Dienst, von dem bekannt ist, dass zumindest der Anbieter die Mails durchliest, für dienstliche, vertrauliche Mails, klicken dann wie Oma Erna auf eine Phishing-Mail und geben den bösen Russen dabei arglos ihre Kennwörter. Und die bösen Russen arbeiten streng nach russischen Arbeitszeiten und veröffentlichen via Wikileaks ein Word-Dokument, das mit einem Programm erstellt wurde, das auf den Gründer der Tscheka registriert ist. Wäre das ein Drehbuch, würde man es mit Fug und Recht als unrealistischen Unsinn bewerten. Dennoch berichten nahezu alle großen Medienerzeugnisse exakt diese Geschichte.

Auch in anderen Fällen, die nicht im Zusammenhang mit dem US-Wahlkampf stehen, und bei denen man „russische Hacker“ verantwortlich machen will, gibt es bestenfalls schwache Indizien; jedoch keinen einzigen Beweis. So beim „Bundestag Hack“ im Jahre 2015, beim Phishing-Angriff auf deutsche Politiker im August dieses Jahres. Selbstverständlich gehören auch Russen zu den Opfern – ganz aktuell macht ein Hackerangriff auf die russische Zentralbank Schlagzeilen. Auch hier ist es völlig unklar, wer die Täter waren.

Cui bono?

Interessant ist, dass keiner der Beteiligten sich zu einer definitiven Aussage hinreißen lässt. Sie werden nirgends lesen, dass „die Russen“ dies oder das gehackt „haben“. Es geht stets nur um Vermutungen, Spekulationen und indirekte Rede. „Aus Sicherheitskreisen heißt es“,

so eine beliebte Formulierung. Ja, wer sind denn diese „Sicherheitskreise“?

Auffällig ist hier, dass nahezu alle Spekulationen, die auf russische Hacker hinweisen, von IT-Sicherheitsunternehmen kommen, deren Geschäftsmodell es ist, Regierungen und Unternehmen vor Cyberkriminalität und Datendiebstahl zu beschützen. Das ist so, als ob die Hersteller von Alarmanlagen und Sicherheitsschlössern wöchentlich vor russischen Einbrecherbanden warnen und dies mit besonders spektakulären Fällen zu untermauern versuchen.

Und Politik und Medien passt das Bild vom „bösen Russen“ natürlich hervorragend ins Bild. Wie kann es nur sein, dass die Wähler nicht der tollen Frau Clinton die Stimme gaben? An einer tiefen Entfremdung zwischen den Wählern und dem politischen Establishment kann es ja nicht liegen … da kramt man dann halt lieber russische Hacker aus dem Hut.

[«*] immer vorausgesetzt, die Schilderungen der Opfer und die veröffentlichten Indizien entsprechen auch der Wahrheit