Die zugreifende Menge

Über Crowdstrike und falsche IT Analysen

#CrowdStrike #DNC #Clinton #FBI

Adler sind ziemlich graziöse Jäger mit geradezu legendären Fähigkeiten, kleinste Beutetiere aus großer Höhe am Boden ausfindig zu machen. Jeder, der einmal die Chance hatte, einen Adler im Sturzflug zu erleben, wie der Greifvogel rasant beschleunigt und mit laser-artiger Präzision zum Boden stürzt, wird den Anblick nicht so schnell vergessen können. Zufälliger Weise hat das IT-Sicherheitsunternehmen mit Namen Crowdstrike genau einen solchen Adler in dessen Firmenlogo. Das Unternehmen wurde 2011 von George Kurtz gegründet, einem ehemaligen CTO des Anti-Viren Softwareherstellers McAfee, sowie Dimitri Alperovich, einem in Russland geborenen IT Sicherheitsexperten und ehemaligen zweiten Chef von McAfee. In Jahre 2012 kam ein ehemaliger FBI Offizieller mit Namen Shawn Henry hinzu, weitere 12 Monate später brachte das Unternehmen sein erstes Produkt mit Namen 'Crowdstrike Falcon' auf den Markt.

Ähnlich zu echten Falken wurde die Software entwickelt, um Computernetzwerke und deren enorme Datenbewegungen bezüglich Eindringlingen und Hackern abzuscannen, die sensitive Informationen, Passwörter und mehr im jeweiligen Netzwerk auszuspionieren beabsichtigen. Nachdem die Firma einige Hackerangriffe aus China, Nordkorea und Russland im Jahre 2014 und 2015 auf großen Unternehmens- und Industrienetzwerken ausfindig machen konnte, erhielt Crowdstrike Investorenzuschüsse u.A. von Google, die sich bis zum Jahre 2019 auf mehr als 480 Millionen US-Dollar bezifferten. Crowdstrike erhielt 2018 eine Marktbewertung von mehr als 3 Milliarden US-Dollar bei Verkaufszahlen von lediglich 100 Millionen US-Dollar und wurde 2019 am NASDAQ gelistet.

Die derzeit drei größten Aktieninhaber von Crowdstrike sind zwei große Silicon Valley Investment-Unternehmen und - komischer Weise - die in München basierte Allianz Asset Management GmbH. Crowdstrikes Markt-Kapitalisierung liegt derzeit bei 15 Milliarden USD bei etwas mehr als 2000 Angestellten, das Unternehmen hat keine Schulden und besaß im Oktober 2019 über 800 Millionen USD an Bargeld zur Verfügung.

Unter all diesen raketenhaften Erfolgsstories mischte sich im Jahre 2016 ein eher rätselhaftes Ereignis, als Crowdstrike einen prallen und farbigen Bericht darüber veröffentlichte, wie eine russische Hackergruppe namens „Fancy Bear" angeblich eine ukrainische Militär App mit Namen „ArtOS" gehackt habe. Die Software kann auf einem Tablet PC installiert werden und wird zur Regulierung von Abschusseinrichtungen genutzt, „um Anpassungen an die Abschusskonditionen von ballistischen und meteorologischen Systemen zu tätigen", so der Entwickler der App, Yaroslav Sherstuk. Crowdstrike machte eine Reihe von global-politischen Aussagen und behauptete in ihrer Bewertung, dass das ukrainische Militär wegen der russischen Hacker „schwere Verluste" in der Feldartillerie erleiden musste.

> Während dieses vorgeschlagenen Entwicklungszeitraums ereigneten sich eine Reihe bedeutender Ereignisse zwischen der Ukraine, Russland und der internationalen Gemeinschaft. Vor allem die russischen Versuche, die Beziehungen zwischen der Ukraine und der EU zu beeinflussen, führten zu einer groß angelegten Protestbewegung am Maidan, die schließlich zum Sturz des damaligen Präsidenten Victor Janukowitsch, zur Invasion und Annexion der Krimhalbinsel durch Russland und zu

> einem langwierigen bewaffneten Konflikt in der Ostukraine führte. Daher wäre die Erstellung einer Anwendung [App], die auf einige der Frontkräfte abzielt und die für die ukrainische Verteidigung an der Ostfront von entscheidender Bedeutung sind, wahrscheinlich eine hohe Priorität für Malware-Entwickler russischer Gegner, die versuchen, das Blatt des Konflikts zu ihren Gunsten zu wenden. Bei ukrainischen Truppen haben Artilleriekräfte auch schwere Verluste auf sich genommen ...
>
> (Crowdstrike Bericht 'Verwendung von Fancy Bear- und Android-Malware bei der Verfolgung ukrainischer Feldartillerieeinheiten')

Seltsamerweise wurden Crowdstrikes Schlussfolgerungen schnell korrigiert. Zum Beispiel vom Internationalen Institut für strategische Studien (IISS), das die folgende Erklärung abgab:

> Der Crowdstrike-Bericht verwendet unsere Daten, aber die aus diesen Daten gezogenen Schlussfolgerungen und Analysen gehören ausschließlich den Autoren des Berichts. Die Schlussfolgerung, dass die Reduzierung der ukrainischen D-30-Artilleriebestände zwischen 2013 und 2016 in erster Linie auf Kampfverluste zurückzuführen ist, ist weder eine Schlussfolgerung, die wir jemals vorgeschlagen haben, noch eine, die wir für richtig halten.
>
> (Stellungnahme von IISS aus dem Jahr 2017)

Ein anderer IISS-Forscher gab an, dass die Reduzierung der Militäreinheiten hauptsächlich auf eine Umverteilung von Einheiten auf andere militärische Kommandos zurückzuführen sei. Das ukrainische Militär berichtete, dass die Artillerieverluste durch die Kämpfe mit den Separatisten in der Ostukraine „um ein Vielfaches geringer waren als die von Crowdstrike gemeldete Zahl und nicht mit der spezifischen Ursache der Hackings zusammenhängen". Der App-Entwickler gab auf Facebook eine Erklärung zu den Ergebnissen von Crowdstrike ab und nannte diese gar „wahnhaft". Er gab zu, dass seine E-Mails kompromittiert waren.

Ebenso interessant ist, dass 2018 ein hochrangiger US Offizieller auf einer Konferenz in Dänemark sich ganz ungeniert darüber ausließ, wie die USA weiterhin die Cybersicherheit der Ukraine mit einem zusätzlichen Gesamtbetrag von 10 Millionen US-Dollar unterstützten - vielleicht ja, um den von Crowdstrike hinterlassenen Unsinn zu bereinigen:

> Während dieser Reise - ich glaube, es war im September letzten Jahres [2017] - gaben wir bekannt, dass wir unsere Hilfsgelder für die Ukraine um 5 Millionen US-Dollar erhöhen, die sich speziell auf die Cybersicherheit konzentrieren. Und als der stellvertretende Sekretär Mitchell im Frühjahr [2018] in die Ukraine reiste, kündigte er zusätzliche 5 Millionen US-Dollar an US-amerikanischen Cybersicherheitshilfen für die Ukraine an.
>
> (Jorgan K. Andrews, Deputy Assistant Secretary, Bureau of International Narcotics and Law Enforcement Affairs im Juni 2018 in Kopenhagen, Dänemark)

Nur wenige Monate vor dem ukrainischen Crowdstrike-Debakel erhielt das Unternehmen im Jahre 2016 vom Democratic National Committee (DNC) die Erlaubnis, deren angeblich russisch-gehackten Computerserver zu untersuchen. Die Polit-Kampagne von Hillary Clinton behauptete damals und übrigens bis heute, dass nicht nur tausende ihrer E-Mails gestohlen wurden - veröffentlicht auf Wikileaks einige Monate vor den US-Präsidentschaftswahlen 2016 - sondern auch ihre gesamte Präsidentschaft.

Es gibt noch mehr widersprüchliche Aussagen und Begebenheiten in Crowdstrikes DNC Serveruntersuchung - nicht begrenzt auf so einige verdächtige und verwirrende Crowdstrike Behauptungen bezüglich Datumswerten, Personen und Methoden - als in der verzogenen Militär-Hacking Angelegenheit in der Ukraine. Das DNC teilte offiziell am 28. April 2016 mit, dass deren Server 'gehackt' worden sei. Trotz der ersten, vom DNC getätigten Zahlungsüberweisung an Crowdstrike am 5. Mai 2016 konnten beide Organisationen nicht verhindern, dass Clinton Emails zuerst in Besitz von Hacker Guccifer 2 gelangten und Ende Juni 2016 auch noch bei Wikileaks veröffentlicht wurden. Die überwiegende Mehrheit dieser Emails, so um die 75%, weist dabei ein Erstellungsdatum von nach der ersten Woche von Mai 2016 auf.

Crowdstrikes CEO Alperovitch behauptet, dass die mit Russland verbundenen Gruppen ein sogenanntes „Powershell.exe" oder „X-Agent" Softwarekommando mit verschlüsselten Parametern verwendet hätten, die sich bei Ausführung in Programmcode verwandeln und die gesamte Verwaltungssoftware des Windows-Betriebssystems steuern können. Der Nachweis, dass solche Befehle tatsächlich von russischen Hackern implementiert worden sind, ist schwierig - wenn nicht fast unmöglich - zu beweisen und hätten ebenso von den vielen westlichen Anti-Trump-Regierungsvertretern implementiert werden können, die wir in deren Unter-allen-Umständen-Trump-zerstören-Agenda in der Vergangenheit erlebt haben.

> Alperovitch verfügt über umfangreiche Erfahrungen als Fachexperte auf allen Ebenen der US-amerikanischen und internationalen Strafverfolgung bei der Analyse, Untersuchung und Profilerstellung transnational organisierter krimineller Aktivitäten und Cyberthreats von terroristischen und nationalstaatlichen Gegnern. Er wird häufig als Experte in nationalen Publikationen zitiert, darunter Associated Press, NBC, New York Times, USA Today und Washington Post.
>
> (Dmitri Alperovitch, Senior Fellow des Atlantic Council)

Eine unabhängige forensische Analyse der Zip-Datei der zuerst von Hacker 'Guccifer 2' in Besitz gelangten Untermenge aller Clinton-E-Mails ergab, dass dessen einzelne Dateien zuletzt zumeist in 2015 abgespeichert wurden, diese über eine langsame Internet-Verbindung am 26. April 2016 exfiltiert, danach auf einen USB-Stick kopiert, von diesem auf einen Computer mit US Ostküsten-Zeitzone kopiert und dort schließlich am 20. Juni 2016 in eine einzige Zip-Datei komprimiert wurden, wenn nicht irgendwie all die Datumsinformationen durch den 'Hack' abgeändert wurden. Dazu sagte CrowdStrikes Präsident und CSO Shawn Henry selbst in einer Anhörung des Ausschusses für die Geheimdienste des US-Kongresses vom 5. Dezember 2017 (auf Seite 32), dass „wir keine konkreten Beweise dafür haben,

dass Daten vom DNC exfiltriert wurden, jedoch haben wir Indikatoren, dass sie exfiltiert wurden".

> **Herr Henry**: "Der Anwalt hat mich nur daran erinnert, dass wir in Bezug auf den DNC Indikatoren dafür haben, dass Daten exfiltriert wurden. Wir hatten keine konkreten Beweise dafür, dass Daten vom DNC exfiltriert wurden, jedoch haben wir Indikatoren, dass sie exfiltriert wurden." (S. 32)
> ...
> **Herr Henry**: "Ja, Sir. Also nochmals, inszeniert, was ich meine, da ist nicht - die Analogie, die ich früher mit Herrn Stewart verwendet habe, war, dass wir kein Video davon haben, aber es gibt Indikatoren, dass es stattgefunden hat. Es gibt Zeiten, in denen wir sehen können, dass Daten exfiltriert werden und wir können es abschließend sagen. In diesem Fall scheint es jedoch so eingerichtet gewesen zu sein, dass sie exfiltriert wurden, aber wir haben einfach nicht die Beweise, die besagen, dass sie tatsächlich herausgegangen sind." (S. 32)
> ...
> **Herr Henry**: "Einige der Daten sahen wir inszeniert, aber wir hatten keinen Hinweis darauf, dass sie exfil't waren, aber sie wurden inszeniert - schienen für exfil inszeniert gewesen zu sein, welche mit Nachforschungen in Verbindung gebracht wurden, die vom DNC über Oppositionskandidaten durchgeführt wurden." (S. 49)
> ...
> **Herr Stewart aus Utah**: "Okay. Sie haben etwas gesagt und ich möchte es noch einmal wiederholen - sagen Sie mir, ob ich falsch liege - wenn ich könnte. Sie sagten, ich glaube, als Sie über den DNC-Computer sprachen, hatten Sie Hinweise darauf, dass Daten für die Exfiltration vorbereitet waren, aber keine Beweise dafür, dass sie tatsächlich herausgegangen sind. Habe ich das richtig aufgeschrieben ?"
> **Herr Henry**: "Ja"
> **Herr Stewart aus Utah**: "Und in diesem Fall sind die Daten, von denen ich annehme, dass Sie davon sprechen, die E-Mails sowie alles andere, was sie möglicherweise versucht haben zu nehmen."
> **Herr Henry**: "Es gab Dateien im Zusammenhang mit Oppositionsforschung, die durchgeführt wurde."
> **Herr Stewart aus Utah**: "Okay. Was ist mit den E-Mails, über die jeder so Bescheid weiß ? Gab es auch Anzeichen dafür, dass sie vorbereitet waren, aber keine Beweise dafür, dass sie tatsächlich exfiltriert wurden ?"
> **Herr Henry**: "Es gibt keine Beweise dafür, dass sie tatsächlich exfiltriert wurden. Es gibt Indizienbeweise - "
> **Herr Stewart aus Utah**: "Okay"
> **Herr Henry**: "- aber keine Beweise dafür, dass sie tatsächlich exfiltriert wurden. Aber lassen Sie mich auch sagen, dass jemand, der einen E-Mail-Server überwacht, auch alle E-Mails lesen kann." (S. 74/75)
>
> Mitschrift des Interviews mit Shawn Henry beim Komitee der Geheimdienste des US Repräsentantenhaus vom 5. Dezember 2017

Darüber hinaus hatte Hillary Clinton in ihrem Privatbüro in Chappaqua, New York einen privaten E-Mail-Server für offizielle Angelegenheiten des US-Außenministeriums verwendet und 2012 sogar Google eingeladen, ihr persönlich-offizielles E-Mail-Konto zu verwalten. Wahrscheinlich, um die Verpflichtung zu umgehen, ihre offiziellen Regierungsgespräche abzusichern und für den Staat zugänglich zu machen. Auf ihrem privaten Server in Chappaqua war eine Windows-E-Mail-Verwaltungssoftware installiert.

Weiter muss man nicht einmal auch nur ansatzweise die Augen eines Adlers haben, um die ziemlich fragwürdigen Sätze des ehemaligen FBI-Direktors James Comey zu erkennen, als er Anfang Januar 2017 im US-Senat nach den DNC-Servern und Crowdstrike befragt wurde:

> **Comey**: „Wir bevorzugen den Zugriff auf das ursprüngliche Gerät oder den betreffenden Server. Dies ist der beste Beweis."
> **Senator**: „Haben Sie forensischen Zugriff auf diese Server erhalten ?"
> **Comey**: „Wir hatten nicht, eine hoch angesehene private Firma [Crowdstrike] bekam schließlich Zugang und teilte uns mit, was sie dort sahen."
> **Senator**: „Ist das normalerweise die Art und Weise, wie das FBI Forensik bevorzugt, oder möchten Sie den Server lieber selbst fühlen und sehen ?"
> **Comey**: „Wir würden es immer vorziehen, selber Zugang zu bekommen wenn das möglich ist."
> **Senator**: „Wissen Sie, warum Ihnen der Zugriff auf die Server verweigert wurde ?"
> **Comey**: „Ich weiß es nicht genau. Ich weiß es nicht genau."
> **Senator**: „Gab es eine Anfrage oder mehrere Anfragen ?"
> **Comey**: „Mehrere Anfragen auf verschiedenen Ebenen und letztendlich wurde vereinbart, dass das private Unternehmen uns mitteilen würde, was sie gesehen hatten."
>
> (Ehemaliger FBI Direktor James Comey bei einer Anhörung im US Senat am 10. Januar 2017)

Es scheint, als ob der DNC mindestens im Jahre 2016 über das FBI bestimmt hat, nicht das US-Justizministerium oder der US-Kongress und/oder US-Senat. Die gesamte DNC-Saga könnte man unter dem Ordner „Massive Korruption" ablegen, wenn da nicht noch US-Präsident Donald Trump am 25. Juli 2019 mit dem neu gewählten ukrainischen Präsidenten Zelensky ein berühmtes Telefonat geführt hätte und in dem der US-Präsident Crowdstrike im Besonderen erwähnte:

> Ich möchte, dass Sie uns einen Gefallen tun, weil unser Land viel durchgemacht hat und die Ukraine viel darüber weiß. Ich möchte, dass Sie herausfinden, was mit dieser ganzen Situation mit der Ukraine passiert ist, man sagt **Crowdstrike**... Ich denke, Sie haben einen Ihrer reichen Leute ... **Der Server, sagen sie, die Ukraine hat ihn**. Es gab eine Menge Dinge, die vor sich gingen, die ganze Situation ... Ich möchte, dass der Generalstaatsanwalt Sie oder Ihre Leute anruft und ich möchte, dass Sie der Sache auf den Grund gehen. Wie Sie gestern gesehen haben, endete dieser ganze Unsinn mit einer sehr schlechten Leistung eines Mannes namens Robert Mueller, einer inkompetenten Leistung, aber sie sagen, dass viel davon in der Ukraine begann.

> (US Präsident Donald Trump im Telefonat vom 25. Juli 2019 mit dem ukrainischen Präsidenten Zelensky)

Bald darauf brach im US-Kongress die Hölle unter zumeist US-demokratischen Politikern aus, die ernsthaft beabsichtigten, den US-Präsidenten wegen diesen Wörtern - plus einigen in Bezug auf Joe Bidens Korruptionsskandalen in der Ukraine - in einem ansonsten angemessenen und normalen Telefonat mit Zelensky aus dem präsidentschaftlichen Amt zu entheben. Das Amtsenthebungs-Theater hielt nicht lange an, es wurde Anfang 2020 endgültig im US-Senat abgelehnt und war ein extrem parteiliches Unterfangen, da alle Republikaner des US-Kongresses es geschlossen auch dort ablehnten.

Es gibt möglicherweise keine andere Erklärung als die, dass die Ukraine tatsächlich irgendwo eine digital gespiegelte Kopie des DNC-Servers hat. Mit möglicherweise ansteckenden Materialien.

Adler können das ganz deutlich von weit oben und von weit entfernt sehen.

https://www.sun24.news/de/die-zugreifende-menge-ueber-crowdstrike-und-falsche-it-analysen.html