15. Jun. 2012

von Martin

in Cyber Security, Sicherheitskultur

Kommentare (6)

Abschreckung durch leaking?

von Martin Schmetz

Die Bombe platzte in der New York Times (Link): Eine wohl platzierte, anonyme Quelle im Weißen Haus bestätigte, dass die USA und Israel hinter Stuxnet steckten. Aber war dieser Leak nur ein weiterer Scoop der NYT oder eine bewusst lancierte Meldung, wie etwa John McCain dem weißen Haus vorwarf? Über die Verkaufszahlen des Buchs zum gleichen Thema muss sich NYT-Redakteur David E. Sanger jedenfalls keine Sorgen mehr machen.

Cybersecurity steht als Thema zunehmend auf der Tagesordnung, sowohl in Deutschland als auch (schon länger) in den USA. Zwei Themenbereiche waren dabei von besonderem Interesse in den letzten Jahren: Leaks auf der einen, Viren und Cyberangriffe auf der anderen Seite. Für letzteres war Stuxnet ein entscheidendes Moment: Ein derart komplexer, scheinbar von staatlicher Hand geschaffener Virus war vorher noch nicht aufgetaucht. Er war mit umfangreichen Wissen angefertigt worden und nur durch eine Fehlfunktion überhaupt ans Licht der Öffentlichkeit gelangt, als er sich unbeabsichtigt stark weiterverbreitete. Selbst die Hackercommunity war voller Anerkennung (etwa hier).

Das von Wikileaks initiierte Cablegate befeuerte die Diskussion um das Phänomen Leaking und Transparenz. Das weiße Haus reagierte entschiedenen und empört, was retrospektiv interessant erscheint: Seit Cablegate wurden viele verschiedene weitere geheime Informationen aus US-Quellen an die Öffentlichkeit gereicht, die Reaktionen aus dem weißen Haus darauf fielen sehr unterschiedlich aus (FP).

Scheinbar gibt es also gute und schlechte Leaks. Der Leak der Stuxnet-Informationen wäre demnach in die Kategorie „gute Leaks“ einzuordnen, denn die Reaktionen auf diesen Leak fielen einigermaßen verhalten aus, bis der politische Gegner sich öffentlich genug echauffiert hatte und schlussendlich doch ermittelt werden musste (link). Fand dieser gewollte Leak (so er denn einer war) nur aus wahlkampfpolitischen Gründen statt, um Obama zusätzliche sicherheitspolitische Kontur zu geben? Oder gab es noch andere Gründe?

Ich glaube, dass es durchaus andere Gründe gab. Wenn Stuxnet tatsächlich eine Cyber *waffe* war, was viele Kommentatoren durchaus so sehen, dann hatte diese mit der Zerstörung der Zentrifugen ihre Aufgabe erfüllt. Technisch war Stuxnet mit der Entdeckung erledigt (Sophos Security): Die ausgenutzten Schwachstellen in Windows und der Steuerungssoftware

SOCIAL MEDIA

SUCHE

Suche...

Suche

TWITTER FEED

Ben Kamis: The concept of #cyberpeace is linguistic trolling. Cyberpeace: post-war is war, only more so http://t.co/fkaHhcgekK #cyberwar
ungefähr 3 Stunden her von &s

Wer wissen will was #cyberpeace ist, sollte wissen was dieser sog. #cyberkrieg ist: Matthias Schulze dazu bei uns http://t.co/LyvFdE29dN
8. Dezember 2014, 11:08 von &s

Neue #Jobs für Politikwissenschaftler_innen! http://t.co/f3vSzfJpMG
5. Dezember 2014, 9:03 von &s

TAGS

wurden behoben, und das Programm ist nun hinreichend bekannt um Gegenmaßnahmen zu entwickeln. Aber wie bei allem im Bereich Cybersecurity gab es das Zuordnungsproblem: Auch wenn die USA und Israel als Urheber vermutet wurden, konnte es nicht schlussendlich bewiesen werden. Die USA, die sich in Konkurrenz zu China, Russland und anderen Staaten im Bereich Cybersecurity sieht, hatte nun die Chance, der an sich erledigten Waffe Stuxnet eine zweite Verwendung zu geben: Zur Abschreckung durch Bekennen. Damit war klar, dass die USA die Möglichkeit zu derartigen Angriffen hat und diese auch tatsächlich durchführt. Und ein inoffizieller Leak hat die angenehme Eigenschaft, offiziell genug zu sein um abschreckend zu wirken, ohne dass jemand dies als staatliche Verlautbarung interpretieren kann um die USA und Israel dann politisch anzugreifen. Ein leak ist eben keine virtuelle Kriegserklärung.

Wichtig ist dabei zu betonen, dass der Vorwurf von Politikern, mit dem Leaking von Stuxnet würden wichtige Geheimdienstkapazitäten öffentlich, damit nicht greift: Die primäre Aufgabe von Stuxnet war nicht das Ermitteln von Informationen, sondern das Zerstören der Zentrifugen. Anders verhält sich dies mit Vorgängern von Stuxnet, die Natanz überhaupt erst auskundschaften sollten, oder dem neuesten "Supervirus" Flame. Das geleakte Bekenntnis zu Stuxnet war in diesem Sinne weniger die Enttarnung eines Spions oder eines Spionageflugzeugs als ein Atomtest: Wir haben die Fähigkeit zur Verwendung solcher Waffen und ihr könnt nichts machen. Seid gewarnt.

Tags: Cablegate, Cyber Spionage, Cyberwar, Leaking, Leaks, Stuxnet, virus

« Happy Birthday, ducklings! Macht der Bilder: Gender und R2P »

6 Kommentare zu "Abschreckung durch leaking?"

Paul | 15. Jun. 2012 um 11:26 | **#1**

Wenn die USA aber zugäben hinter Stuxnet zu stecken ist der Einsatz von Stuxnet nicht mehr so sehr einem Atomtest gleichzusetzen. Das wäre der Fall wenn sie die mit Stuxnet ihre eigenen Zentrifugen kaputt gemacht hätten. "Atomtests" in fremden Ländern werden gerne mal als Krigshandlung gewertet. Was natürlich der Grund sein wird aus dem die Verantwortung für Stuxnet und damit die zerstörten Zentrifugen nur inoffiziell durch den vermeintlichen Leak übernommen wird.

ANTWORTEN

seditioni | 15. Jun. 2012 um 13:32 | **#2**

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science! Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier Raum sein

Deutschlands Irak-Politik – Verantwortung nach außen, Intransparenz nach innen.

Wir haben Geburtstag!

„Mit Sicherheit nicht!" Sexuelle Gewalt als politisches Mittel

KATEGORIEN

Außenpolitik (59)
Bürgerkriege (16)
Cyber Security (42)
Demokratisierung (9)
Drohnen (15)
Humanitäre Interventionen (15)
Innere Sicherheit (24)
Interviews (10)
Katastrophen (4)
Konferenz (20)
Militär (28)
Pandemien (2)
Podcast (7)
Popkultur (21)
Sanktionen (8)
Security Culture (14)

Ich denke, es ist hier auch der Atomtest auf eigenem Gebiet gemeint, also die Demonstration gewisser Waffen oder Fähigkeiten zur Abschreckung anderer. Aber ja, Stuxnet ist ein gezielter Angriff und daher geschah vllt wirklich der Weg über leaking statt öffentlicher Bekennung und damit einhergehender Verantwortung.

ANTWORTEN

literally | 15. Jun. 2012 um 16:27 | **#3**

Guter Punkt. Die Idee war eigentlich, dass durch einen Angriff allein kein Abschreckungspotenzial entstehen kann, weil der Angriff ja nicht eindeutig zuzuordnen ist. Man kann dieses Potenzial nur erreichen, wenn man sich anschließend dazu bekennt. Aus den von Dir genannten Gründen natürlich eher durch die Blume.
Ich denke aber, dass Du auf zwei wichtige Dinge hinweist, die man (in einem weiteren Post) noch einmal näher ausführen sollte: Nämlich erstens, dass die technologische Fähigkeit allein im Kontext von Cybersecurity offensichtlich kein Abschreckungspotenzial hat. Man kann, wie du sagtest, auf eigenem Gebiet Atombomben testen und schickt damit eine klare Botschaft. Beim Gegner würde man einen solchen Test eher nicht durchführen; jedenfalls wäre es dann kein Test. Würde man sich damit brüsten, dass man seine eigenen Netze geknackt oder sogar Anlagen durch Hacks oder Viren zerstört hat, hätte dies vermutlich kein Abschreckungs- sondern höchstens Verwunderungspotenzial. Abschreckung kann also im Kontext der Cybersecurity glaubwürdig nur durch einen geglückten Angriff oder zumindest die Veröffentlichung beeindruckender Exploits o.Ä. geschehen.
Das führt mich dann auch zum zweiten Punkt, nämlich dass ein Angriff im Netz (im Gegensatz zu konventionellen Waffen) offensichtlich einen bedeutend niedrigeren Stellenwert hat. Hoch genug, als dass man sich nicht wirklich offiziell damit brüsten will, aber klar zu niedrig als dass das außerhalb diplomatischer und elektronischer Dimensionen ernsthafte Konsequenzen haben würde.

ANTWORTEN

Cem | 16. Jun. 2012 um 10:10 | **#4**

Eine sehr schöne Analogie, leaking durch Abschreckung. Das ist dann mit Israels Atomwaffen vergleichbar: Alle wissen davon, die Abschreckung entfaltet Wirkung, aber richtig eingestehen und die Konsequenzen tragen (NPT etc.), müssen die Regierungen nicht.

ANTWORTEN

janusz | 16. Jun. 2012 um 20:13 | **#5**

Gute Idee! Angenommen die Verlautbarung der Verantwortung der USA und Israels für Stuxnet war ein lancierter Leak, wirft dieser Vorgang tatsächlich einige interessante Fragen auf.
Tatsächlich kann man argumentieren, dass das Leaken eine abschreckende Wirkung haben könnte, da es die implizte Drohung enthält, dass die Fortführung des iranischen

Sicherheits-Kommunikation (14)
Sicherheitskultur (205)
Sozialwissenschaft Online (57)
Stellenangebote (42)
Strategie (10)
Terrorismus (14)
Theorie (2)
Umwelt (1)
Versicherheitlichung (22)
Visualisierung (5)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (48)

BLOGROLL

Arbeitskreis soziale Bewegungen
Augen geradaus
Dan Drezner
Dart-Throwing Chimp
David Campbell
de.hypotheses.org
Demokratieforschung Göttingen
Duck Of Minerva
Future and Politics
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps

Atomprogramms zu derartigen Angriffen führen kann, da beispielweise die USA und Israel in der Lage und Willens sind, potente Cyberwaffen zu produzieren und einzusetzen. Der Angriff mit Stuxnet verleiht dieser impliziten Drohung eine gewisse Glaubwürdigkeit. Aber erstens: Sind derart implizite Drohungen tatsächlich glaubwürdig? Oder bedarf es expliziter Drohungen um glaubwürdig abzuschrecken (Beispiel: US Sicherheitsstrategie)? Zweitens: Stuxnet war ein gezielter Angriff auf eine bestimmte Einrichtung. Es ist fraglich, ob die Androhung gezielter Attacken ("discriminate force") eine solche Abschreckungswirkung haben kann, wie die Anwendung unterschiedsloser Angriffe (indiscriminate force"). Die Kosten eines gezielten Angriffs sind nicht besonders hoch. Cyberangriffe mit hohen Kosten könnten zum Beispiel Angriffe auf die Infrastruktur eines ganzen Landes sein (Strom, Wasser).
Wohlmöglich wäre es interessant etwas eingestaubte Beiträge zur Debatte über "nuclear deterrence" hervorzukramen und die Ideen von damals auf Cybersecurity heute zu übertragen. Thomas Schellings "The strategy of conflict" bietet sich hier beispielsweise an.

ANTWORTEN

seditioni | 16. Jun. 2012 um 21:24 | **#6**

@Cem: Man kann es ja gerade nicht mit konventionellen Waffen vergleichen, da das tatsächliche Risiko, im Gegensatz zu Atombomben, unbekannt ist.
Daher wäre es, da stimme ich Janusz zu, interessant zu untersuchen, welche Wirkung implizite Drohungen haben.
Dass sie aber keinerlei Abschreckungspotenzial haben, denke ich nicht, auch wenn die Herkunft von schädlichen Viren nicht völlig geklärt ist. Schließlich ist bekannt, dass die USA auf den Feldern "Cybersecurity" und "Cyberwaffen" va seit einigen Jahren verstärkt forscht – wenn dann gefährliche Viren auftauchen und, wenn auch durch nicht bestätigte Leaks, Verbindungen zu den USA hergestellt werden, reicht dies für eine Abschreckung meiner Meinung nach aus. Welche Wirkung eine solche 'gefühlte' oder 'implizite Bedrohung' im Gegensatz zu anderen, expliziten, hat, und welche Konsequenzen sie nach sich zieht (oder eben auch nicht), wäre eine spannende Frage.

ANTWORTEN

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Kings Of War
netzpolitik.org
percepticon
shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat

Geben Sie den Text ein.

reCAPTCHA

Bestätigen

Datenschutz - Nutzungsbedingungen

Kommentar senden

☑ Benachrichtige mich über nachfolgende Kommentare per E-Mail.

(cc) BY-NC-ND

Dieses Werk bzw. Inhalt steht unter einer Creative Commons Namensnennung-NichtKommerziell-KeineBearbeitung 3.0 Unported Lizenz.
Über diese Lizenz hinausgehende Erlaubnisse können Sie unter redaktion@sicherheitspolitik-blog.de erhalten